Personnel Clearances in the NISP

Student Guide

August 2016

Center for Development of Security Excellence

Lesson 1: Course Introduction

Course Introduction

Course Information

Welcome to the Personnel Clearances in the National Industrial Security Program (NISP) Course.

Item	Explanation
Purpose	Provide a thorough understanding of the personnel security clearance request process and maintenance for cleared contractors who participate in the NISP
Audience	• DoD Industrial Security Specialists • Contractor Facility Security Officers • Other security practitioners in the NISP
Pass %/Fail	75% on final examination
Estimated completion time	105 minutes

Course Overview

The federal government often contracts with private industry for goods and services. Sometimes those contracts require the government to allow industry contractors access to classified information. Controlling access to classified information by implementing a personnel security program (PSP) at cleared facilities is essential to protecting our national security.

This course will review the regulatory basis for the personnel security program. As an important part of the PSP, this course will also discuss the process to obtain a personnel security clearance (PCL). The contractor's responsibility under the PSP does not end with the issuance of a PCL eligibility determination. Therefore, this course will identify the activities necessary to maintain a PCL and manage the PSP at a cleared contractor facility.

Course Objectives

Here are the course objectives:

- Identify the legal and regulatory basis of the personnel security program
- Identify key terms relating to personnel security
- Identify the role of various organizational components (PSMO-I, DoD CAF, DOHA) in the NISP personnel security clearance process for industry contractors

- Identify contractor, applicant, and government responsibilities in the processing of personnel security clearance eligibility
- Identify the basic and common functions of the DoD system of record, including the systems' use of the terms "eligibility" and "access"
- Identify the revised Federal Investigative Standards (FIS) used to make national security eligibility determinations
- Identify the adjudicative standards for the personnel security program
- Identify key elements of the management of the personnel security program at a cleared facility

Course Structure

This course is organized into the lessons listed here:

- Course Introduction
- Overview of Personnel Clearances in the NISP
- Processing PCL Eligibility
- Managing the PSP at a Cleared Facility
- Course Conclusion

Lesson 2: Overview of Personnel Clearances in the NISP

Lesson Introduction

Objectives

In order for the government to entrust individuals with classified information, the government must ensure that those individuals are loyal, trustworthy, and reliable. When such individuals are contractor personnel, personnel security is governed by the National Industrial Security Program (NISP). Implementing personnel security to manage access to classified information is key to the protection of national security.

In this lesson, you will learn about personnel clearances in the NISP. You will identify key terminology related to the personnel security program (PSP) and to personnel security clearances (PCLs). You will examine the roles of important organizational components in the NISP PCL process. You will also examine the legal and regulatory basis of the PSP.

Here are the lesson objectives:

- Identify key terms relating to personnel security
- Identify the role of various organizational components (PSMO-I, DoD CAF, DOHA) in the NISP personnel security clearance process for industry contractors
- Identify the legal and regulatory basis of the personnel security program

Purpose of the Personnel Security Program

Introduction to the NISP

The personnel security program (PSP) protects national security by ensuring that all individuals with access to classified information are loyal, trustworthy, and reliable. The defense contractor aspect of the PSP is overseen by the NISP. Under the NISP, which was established by Executive Order 12829, the federal government works together with private industry to ensure that classified information entrusted to industry is protected. The Facility Security Officer (FSO) plays a major role in this cooperation by developing and implementing a facility's security program.

Eligibility and Access

Before contractor personnel may access classified information, they must be granted a personnel security clearance (PCL) to ensure that access to classified information is in the best interest of national security. To obtain a PCL the FSO at the contractor facility must determine that access to classified information will be needed for the individual to perform his or her duties. If this is the case, the individual must also be granted a favorable eligibility determination.

To be granted eligibility, contractor personnel must first undergo a background investigation. Then a trained government adjudicator will review the background investigation material and determine whether granting the individual access to classified information would be consistent with national security. This combination of a favorable eligibility determination, and the determination that classified access will be needed in order for the individual to perform his or her duties, makes up a PCL.

It is important to note, however, that just because an individual is granted eligibility does not mean he or she may have access to classified information. In order to actually access a particular piece of classified information, an individual must have not only a PCL, but also a clear need to know the specific classified information being accessed. Typically, an individual's need to know is based on the requirement to access specific classified information in the performance of duties on a classified contract.

Personnel Security Clearances and the NISP

The PSP in the NISP

As you learned, although the NISP is a compliance program, the program relies on a partnership between the federal government and industry contractors to ensure we continually work together to protect classified information. The Personnel Security Program helps ensure that protection.

In order to understand how the PSP operates within the NISP, you need to understand the roles of the government entities involved, as well as the role of the contractor. Let's take a look at organizational components of both the federal government and the contractor in the NISP.

Government Components

There are many entities involved in the NISP; however, a few organizational components are particularly relevant to personnel security clearances. Let's take a look.

Cognizant Security Agencies (CSAs) establish and monitor security programs within the NISP. The Department of Defense (DoD) is one of five CSAs operating under the NISP, and it represents 31 other federal agencies and departments in this capacity. A Cognizant Security Office (CSO) is responsible for the administration and implementation of security-related activities under the NISP.

The Defense Security Service (DSS) is the CSO for the DoD. Within DSS there are two operational units that work directly with personnel at contractor facilities: the Personnel Security Management Office for Industry (PSMO-I) and the DSS Field Office. The PSMO-I office is vested with worldwide responsibility under the NISP for processing and tracking applications for industrial personnel security clearances, and performs as the Cognizant Government Authority for personnel security management and oversight under the NISP. Within the DSS Field Office, Industrial Security Representatives (IS Reps) work directly with their assigned contractor FSOs to ensure that classified information entrusted to contractors is protected.

The PSMO-I office is vested with worldwide responsibility under the NISP for processing and tracking applications for industrial personnel security clearances, and performs as the Cognizant Government Authority for personnel security management and oversight under the NISP.

The other DoD organizations which are involved in the clearance adjudication and appeals process are the Department of Defense Consolidated Adjudications Facility (DoD CAF) and the Defense Office of Hearings and Appeals (DOHA). The primary responsibility of the DoD CAF is making personnel security clearance eligibility determinations through the adjudication of personnel security background investigations. The DoD CAF can grant or deny eligibility. If the DoD CAF denies the eligibility, the decision can be appealed to DOHA which provides hearings and issues decisions in personnel security clearance cases for contractor personnel.

Contractor Components

Within a cleared contractor facility, several individuals play an important role in personnel security.

The FSO oversees the facility's security program and works directly with government components involved in the NISP. In addition, key management personnel (KMP) are those individuals with the authority and responsibility for planning, directing, and controlling the activities of a company. KMP include owners, officers, and directors of the company and its operations, as well as executive personnel at the contractor facility including the FSO.

Note that in order to be approved as a cleared facility, contractors must obtain a facility security clearance (FCL) which is an administrative determination that a facility is eligible to access classified information. In order to obtain an FCL, essential KMP must receive a personnel security clearance eligibility determination.

Communicating PCL Information

Now that you know the organizational components involved in operating the PSP within the NISP, let's take a look at how these different entities communicate with one another regarding PCLs. The Joint Personnel Adjudication System (JPAS) is the DoD system of record that has connected FSOs and other security program managers with a single database for managing and maintaining personnel security clearance eligibility and access information.

JPAS indicates if an individual has eligibility. A subsystem of JPAS is the Joint Clearance and Access Verification System (JCAVS). JCAVS allows the contractor to access and update PCL information, thereby ensuring reciprocity. If an individual does not have eligibility, then the contractor can initiate the process to obtain an eligibility determination using JPAS.

It is important to note that a new DoD system, the Defense Information System for Security (DISS) is replacing JPAS. DISS consists of two main components, the Case Adjudication Tracking System (CATS) and the DISS Portal which is taking the place of JCAVS.

The contractor employee then uses Electronic Questionnaires for Investigations Processing (e-QIP) to complete the Questionnaire for National Security Positions, also referred to as SF-86.

Legal and Regulatory Basis

Personnel Security Clearances

Even professionals trained in processing PCLs may sometimes have questions. Let's examine a few resources that may assist you when you have questions about PCLs.

Executive Order 12968 provides policy about PCLs and defines the requirements for accessing classified information, however, the resource most useful to an FSO is DoD 5220.22-M, commonly referred to as the National Industrial Security Program Operating Manual (NISPOM). This manual provides guidance to FSOs about how to implement PCL policy and details requirements for PCLs issued under the NISP.

Meet Brenda Taylor. She's a new hire at a cleared contractor company called Belacort Industries. Brenda's project manager notifies Belacort's FSO, Ted Fuller, that Brenda will require access to classified information, so Mr. Fuller asks to meet with Brenda to discuss the PCL process. Because this is Brenda's first PCL investigation, she asks Mr. Fuller to explain the standards and guidelines for deciding her eligibility determination. Mr. Fuller consults the Adjudicative Guidelines, which provide the adjudicative standards and guidelines for the NISP PCL process, and explains the criteria to Brenda. These resources are good references to have access to as an FSO administering a personnel security program for a cleared facility.

Review Activity

Review Activity 1

For each question, select the best answer. Check your answers in the Answer Key at the end of this Student Guide.

1 of 4: _____ is vested with worldwide responsibility under the National Industrial Security Program (NISP) for processing and tracking applications for industrial personnel security clearances..

- ○ DoD CAF
- ○ PSMO- I

2 of 4: _____ typically determines personnel security clearance eligibility of contractor employees.

- ○ DoD CAF
- ○ DOHA

3 of 4: _____ processes and tracks applications for industrial personnel security clearances, and performs as the Cognizant Government Authority for personnel security management and oversight under the NISP.

- ○ PSMO- I
- ○ DOHA

4 of 4: _____ decides unfavorable eligibility determinations that are appealed.

- ○ DoD CAF
- ○ DOHA

Review Activity 2

Indicate who uses each system or secure website for each statement. Check your answers in the Answer Key at the end of this Student Guide.

1 of 3: Retrieves DoD PCL eligibility information in the DoD system of record

- ○ FSO
- ○ Contractor Employee

2 of 3: Initiates PCL investigation requests from the DoD system of record

- ○ FSO
- ○ Contractor Employee

3 of 3: Completes the Questionnaire for National Security Positions using e-QIP

- ○ FSO

- ○ Contractor Employee

Review Activity 3

Indicate which regulation or resource matches each description. Check your answers in the Answer Key at the end of this Student Guide.

1 of 3: Used in the PCL process to help in determining a candidate's eligibility

- ○ E.O. 12968
- ○ NISPOM
- ○ Adjudicative Guidelines

2 of 3: Provides policy about PCLs and defines the requirements for accessing classified information

- ○ E.O. 12968
- ○ NISPOM
- ○ Adjudicative Guidelines

3 of 3: Provides requirements regarding PCLs among other aspects of the NISP

- ○ E.O. 12968
- ○ NISPOM
- ○ Adjudicative Guidelines

Lesson 3: Processing NISP PCL Eligibility

Lesson Introduction

Objectives

The personnel security clearance (PCL) process is complex and involves a great deal of communication between the contractor and the government.

In this lesson, you will learn about the responsibilities of both the contractor and government in the NISP PCL process. You will identify the common functions of the DoD current system of record.

You will learn about the new Federal Investigative Standards (FIS) as well as the legacy personnel security investigations used to make personnel security clearance eligibility determinations on contractor employees in the past.

You will also identify the adjudicative standards for the personnel security program (PSP).

Here are the lesson objectives:

- Identify contractor, applicant, and government responsibilities in the processing of personnel security clearance eligibility
- Identify the basic and common functions of the DoD system of record (currently JPAS), including the system's use of the terms "eligibility" and "access"
- Identify the revised Federal Investigative Standards used to make national security eligibility determinations

Overview of the NISP PCL Process

Processing a Request for a PCL

Requesting, processing, and receiving a PCL involves four stages. Once the determination is made that an employee or prospective employee requires access to classified information to perform his or her duties, the contractor initiates the PCL request process. The Personnel Security Management Office for Industry (PSMO-I) reviews all Questionnaires for National Security Positions, referred to as SF 86s, for completeness, validates the need and clearance level requested and reviews for possible interim clearance consideration pending an investigation of the candidate. The investigative service provider, often the Office of Personnel Management (OPM) performs any necessary agency checks, and when applicable, conducts interviews. Then the investigation results are evaluated by the Department of Defense Consolidated Adjudications Facility (DoD CAF) and an eligibility determination is made.

Initiation of the NISP PCL Process

Overview of Initiation Activities

Initiating the personnel security clearance process involves six steps. First, the facility security officer (FSO) verifies the candidate's citizenship and reviews the DoD system of record for any pre-existing record of the candidate. If the candidate does not have a valid pre-existing clearance, the FSO uses the DoD system of record to initiate the PCL request. Then, the candidate completes the SF-86. Once the candidate has completed the SF-86, the FSO reviews the security package and, if everything is in order, submits the security package. Let's take a look at each of these activities in more detail.

FSO Use of DoD System of Record

Prior to initiating the NISP PCL process, the FSO verifies that the candidate is a U.S. citizen by examining either the candidate's birth certificate, passport, or any of the other documents listed in NISPOM section 2-208. Note that those forms of identification accepted as part of the I-9 Employment Eligibility Verification form are not sufficient for this purpose, and neither may the FSO use the DoD system of record to verify a candidate's citizenship. A candidate's citizenship must be verified only if it is the candidate's initial personnel security clearance investigation. The FSO then reviews the DoD system of record to assess if a new investigation to determine eligibility needs to be initiated. There are three aspects the FSO seeks to review in the DoD system of record.

First, the FSO determines whether or not the candidate has a record present in the DoD system of record. Then, if the candidate does have a record in the DoD system of record, the FSO identifies whether or not the candidate has a pre-existing favorable eligibility determination. Finally, if the candidate does have a pre-existing favorable eligibility determination, the FSO assesses whether or not that determination may be accepted in lieu of initiating a new investigation to determine eligibility. If a candidate has no record in the DoD system of record and therefore no pre-existing eligibility determination, then the FSO will establish a record of the candidate in the DoD system of record and initiate a PCL request. If the candidate does have a record in the DoD system of record but does not have a pre-existing eligibility determination, then the FSO will initiate a PCL request for the candidate using the DoD system of record. If the candidate has a record in the DoD system of record and has a pre-existing eligibility determination, then the FSO will review the record in the DoD system of record to assess whether the determination may be accepted in lieu of a new investigation, or if a new investigation is required to determine eligibility.

Let's take a look at what factors the FSO evaluates to make such a determination.

Evaluating a Pre-Existing Eligibility Determination

A pre-existing favorable eligibility determination may be accepted whether it was issued by the federal agency currently requiring the candidate to be cleared, in this case the DoD, or by a different federal agency. The mutual acceptance of a favorable eligibility determination issued from one federal agency by a different federal agency is called reciprocity. Title 32 of the Code of Federal Regulations Part 148 and Section 2-201 of the NISPOM establish the requirements for reciprocity.

If a pre-existing favorable eligibility determination meets or exceeds the requirement for reciprocity, then no PCL request is needed. If a pre-existing eligibility determination does not meet or exceed the requirement, then the FSO will need to initiate a PCL request.

PCL Request NOT Needed

If a prior investigation or personnel security eligibility determination is made by a federal agency and it meets the investigative scope and standards of the NISPOM required for the needed personnel security clearance eligibility level, then that investigation or eligibility determination may be accepted by a different federal agency for investigative or clearance purposes provided all of the following conditions are met.

First, the previously granted eligibility determination must be based upon an investigation that is current within 5 years. Second, an inquiry with the issuing agency discloses no reason why the eligibility determination should not be accepted. And third, no break longer than 24 months exists in the candidate's relationship with the issuing agency since completion of the prior investigation.

PCL Request Needed

The candidate's FSO will need to initiate a new PCL request if the pre-existing investigation or eligibility determination fails to meet any one of the required conditions.

Candidate Use of e-QIP

Remember Brenda, the new contractor employee who needs a PCL? To initiate the clearance process Brenda's FSO, Mr. Fuller, checks the DoD system of record and determines that she does not have a record in that system, nor does she have a pre-existing eligibility determination. Therefore, he establishes a record for Brenda in the DoD system of record and initiates a PCL request to obtain a personnel security clearance eligibility for her. Brenda can now use the Electronic Questionnaires for Investigations Processing (e-QIP) to complete the SF-86.

Once she has completed the SF-86 and submitted it electronically for review by her FSO, Brenda must print and sign the SF-86 Certification Page, the Authorization for Release of Information and Records, and the Fair Credit Reporting Disclosure Authorization, and provide them to Mr. Fuller so that he can review her security clearance package. Additionally, if the applicant answered "Yes" to item 21 of the SF-86, Mental and Emotional Health, she may need to sign and submit the Authorization for Release of Medical Information.

FSO Review of Security Clearance Package

Now that Brenda has completed the SF-86 and submitted the signed SF-86 certification page, signed authorization and release form, and signed credit disclosure authorization to Mr. Fuller, he can perform an FSO review of Brenda's security clearance package. As specified in NISPOM paragraph 2-202, a candidate's FSO must review the completed SF-86 to determine its adequacy and completeness. The NISPOM explicitly states that the sole purpose of an FSO's review of the SF-86 is

to ensure adequacy and completeness, and that the information contained in a candidate's security clearance package cannot be used for any other purpose. The FSO must also provide a written notification assuring the candidate of these constraints. Guidance on how to perform an FSO review of the SF-86 is available from the Defense Security Service website. The written notification reads as follows, "The scope of this review is limited to determining the adequacy and completeness of your SF-86. The information contained in your SF-86 cannot be used by Belacort Industries for any purpose other than to determine the adequacy and completeness of your security clearance package."

Submission of the Security Clearance Package

Mr. Fuller reviewed Brenda's security clearance package and determined that it was adequate and complete. Now, he must submit the package to PSMO-I. Using the DoD system of record, Mr. Fuller can review and submit Brenda's SF-86 electronically. Copies of the signed certification and release forms must be scanned and transferred into electronic copies which are then submitted as attachments in the DoD system of record. Handwritten comments may be made on the scanned copies if needed; however, PSMO-I recommends against making annotations.

Retention of the Security Clearance Package

Copies of the documents included in the security clearance package are submitted to PSMO-I, but what is done with the originals? According to the NISPOM, the FSO must retain the original signed copies of the SF-86 and both certification and release forms until the clearance process has been completed. Once the applicant's request for eligibility to access classified information has been granted or denied, the retained documentation must be destroyed or returned to the applicant to maintain. Because the SF-86 is reviewed as part of Special Access Program (SAP) access determinations, the most current SF-86 for individuals approved for, in process to receive, or who may be considered for nomination to receive SAP access may be retained by the cleared contractor facility for SAP access purposes after completion of the PCL process.

Interim Reviews

Overview of Interim Reviews

Once the NISP PCL process has been initiated, and the applicant's security clearance package has been submitted, the second stage of the PCL process may begin. In the second stage of the PCL process, an interim review of the security clearance package is conducted to determine whether the applicant will be granted an interim eligibility determination. Once an interim eligibility determination has been made and the PSMO-I has released the security clearance package to the investigative service provider (ISP), in this case it is the Office of Personnel Management (OPM), the FSO will submit a fingerprint card if appropriate.

Interim Review Process

All applicants for a PCL submitted by a cleared contractor are routinely considered for interim eligibility. Interim eligibility permits the applicant to have access to most of the classified information needed to perform his or her duties. The interim eligibility determination is made concurrently with the initiation of the investigation and generally remains in effect until the investigation is completed. Not all applicants are granted interim eligibility.

Fingerprint Cards

If after completing an interim review there is no apparent reason why the candidate is ineligible at this time, and the security clearance package is released to OPM, then the FSO may forward the candidate's fingerprint card, if one is required. Because this is Brenda's first investigation, a fingerprint card will need to be submitted in addition to her security clearance package. Note that fingerprint cards are not submitted for periodic reinvestigations. Fingerprints must be submitted electronically to OPM. If the electronic fingerprint card is not received within 14 days of the investigation request being received by OPM, the investigation request will be rejected.

Policy Change

Effective October 1, 2016, all fingerprints associated with SON 346W must be submitted electronically to OPM or the fingerprint will be rejected. If an electronic fingerprint is not received within 14 days of the investigation request being received by OPM, the investigation request will be rejected.

The Under Secretary of Defense for Intelligence issued a requirement for DoD Components to begin transitioning to electronic capture and submission of fingerprint images in support of all background investigations by December 31, 2013. The National Industrial Security Program (NISP) is among the leading Components in submitting electronic fingerprints to Secure Web Fingerprint Transmission (SWFT) application with more than 6,500 electronic fingerprints submitted to OPM in December 2015 and less than one percent, or just 99 fingerprint cards, submitted in hardcopy. PSMO-I will be contacting the FSO and Requesting Official of recent companies submitting hardcopy fingerprints in order to close the gap and achieve 100 percent electronic submission.

Personnel Security Investigations

Overview of Personnel Security Investigations

Once a determination has been made regarding whether to grant the applicant interim eligibility, the third stage of the NISP PCL process may begin. In the third stage of the PCL process, the ISP conducts the appropriate background investigation. The ISP begins by confirming that the security clearance package is complete. Next, the ISP carries out the investigation by verifying the information contained in the package, pursuing any leads prompted by a review of the information in the package, and conducting interviews when appropriate.

Reviewing for Completeness

The ISP, in this case OPM, has received Brenda's security clearance package. Before beginning Brenda's investigation, OPM must first confirm that her security clearance package is complete. In this case, Brenda's security clearance package contains all the required components, so OPM may commence a personnel security investigation. If, however, all the required components of the security clearance package had not been received within 30 days of OPM's receipt of the package, then OPM would have returned the package. Upon receipt of the returned security clearance package, the applicant is contacted by the FSO and provided instructions on the steps required to resume processing.

Initial Investigations

Since OPM has received Brenda's security clearance package and fingerprint card and determined them to be complete, it will now conduct a background investigation of Brenda. In a basic background investigation, OPM as the ISP will check national agency records, including fingerprint records, when appropriate, and verify the information provided by the applicant such as addresses, employers, and schools. The ISP will also contact neighbors, supervisors and co-workers, classmates, and references, if required, and contact law enforcement agencies in the places where the applicant lived, worked, and attended school. Further, the ISP investigator will explore any investigative leads identified during the review of the security clearance package. Finally, the investigator will conduct a personal interview with the applicant, if required by the investigation type.

Five-Tiered Investigative Model

On June 30, 2008, President George W. Bush signed Executive Order 13467. This executive order calls for an efficient, reciprocal, and aligned system to be used across the government to investigate and determine: eligibility for logical and/or physical access to federally controlled facilities and information systems, also known as Homeland Security Presidential Directive 12 (HSPD-12); suitability for federal employment and fitness to perform work on behalf of the Federal Government as a contractor employee; and eligibility for access to classified information, or to hold a sensitive position.

In December 2012, revised Federal Investigative Standards (FIS) were approved by James Clapper, the Director of National Intelligence (DNI), and John Berry, the former Director of the Office of Personnel Management (OPM). The revised FIS established a new investigative model, which aligns and standardizes background investigation requirements for HSPD-12, suitability and fitness, and national security, into 5 tiers. This new 5-tiered model facilitates reciprocity, uses a build-upon, but not duplicate, investigative principle, and facilitates the use of automation to improve cost, quality and timeliness of background investigations. OPM is responsible for conducting investigations at all five tiers. Tiers 3 and 5 are the investigations used for PCLs to grant eligibility to classified information and/or assignment to a national security sensitive position. The revised investigative standards are being implemented in phases with final implementation for all tiers anticipated by

October 2017. If you would like to know more information about the FIS implementation timelines, please see the 2012 Revised Federal Investigative Standards Crosswalk.

Tier 3

Tier 3 Investigations are conducted for National Security Adjudications for positions designated as non-critical sensitive, and/or requiring Confidential, Secret or "L" access eligibility. The Standard Form (SF) -86 is the investigative form used for Tier 3 investigations.

Tier 5

Tier 5 investigations are conducted for National Security Adjudications for positions designated as critical-sensitive or special-sensitive and/or requiring "Q" or Top Secret access or access to Sensitive Compartmented Information (SCI). The Standard Form (SF) -86 is the investigative form used for Tier 5 investigations.

Periodic Reinvestigations

In addition to initial investigations, some positions require periodic reinvestigations by OPM. Under the new Federal Investigative Standards, a reinvestigation is required at least every five years for Tiers 2, 3, 4 and 5. Tier 1 does not have a mandatory reinvestigation requirement. While the new 5 year reinvestigation requirement is not a change for continuing Top Secret eligibility, it does replace the old investigative requirement of having a periodic reinvestigation every 10 years for continuing Secret eligibility and every 15 years for continuing Confidential eligibility.

Former Background Investigations

The new 5-tiered investigative model is replacing several investigations that were previously used to make security clearance determinations. Although these initial and periodic investigations are being phased out, you should be aware of the investigations being replaced by Tiers 3 and 5.

Tier 3 replaces the Access National Agency Check with Inquiries (ANACI) which was the initial investigation used for civilian federal employees who were assigned to noncritical-sensitive positions and/or required eligibility for access to Confidential or Secret information. And it also replaces the National Agency Check with Law and Credit Checks (NACLC) which was the initial investigation for members of the military and contractors requiring eligibility for access to Confidential or Secret information. The NACLC was also the appropriate periodic reinvestigation for continuing Confidential and Secret eligibility and/or continued assignment to non-critical sensitive positions for everyone.

Tier 5 replaces the Single Scope Background Investigation (SSBI) which was used for granting initial eligibility for assignment to Special-Sensitive or Critical-Sensitive positions and/or Top Secret or SCI clearance eligibility. It also replaces the SSBI-Periodic Reinvestigation (SSBI-PR) and Phased Periodic Reinvestigation (PPR) which were used to grant continuing Top Secret and SCI eligibility and/or assignment to Special-Sensitive or Critical-Sensitive positions.

Adjudications

Overview of Adjudicative Process

After the ISP has completed the applicant's personnel security investigation, the fourth stage of the NISP PCL process may begin. In the fourth stage of the PCL process, the results of the background investigation are forwarded to the DoD CAF. The DoD CAF will evaluate the investigative results using the "whole person concept" and the 13 adjudicative guidelines to make an adjudicative decision. Once the adjudicative decision has been made, the applicant will be notified.

The Whole Person Concept

In order to conduct a review that is fair and free of bias, adjudicators use the "whole person" concept to determine whether or not to grant eligibility. The whole person concept involves carefully assessing all the available information about an applicant, both favorable and unfavorable, from the applicant's past and in the present. The applicant's strengths are evaluated to determine whether they outweigh any weaknesses. This careful evaluation of favorable information and unfavorable information, from a subject's past and present, takes the whole person into consideration.

Adjudicative Guidelines

Adjudicators evaluate applicants using a standardized set of thirteen guidelines to ensure that all applicants are assessed using the same criteria in a manner that is fair and free of bias. These guidelines are applied using the whole person concept, meaning that when an applicant is reviewed under a guideline, both disqualifying and mitigating information is considered. Each guideline addresses a specific concern that can impact a candidate's ability to protect national security. Review each guideline below to learn about the concern associated with it. For more information about the adjudicative process, refer to the Adjudicative Desk Reference.

Term	Definition/Explanation	Concern
Guideline A	Allegiance to the U.S.	An individual who wants to bring about change through unconstitutional, unlawful, or violent means may compromise national security in the furtherance of their cause.
Guideline B	Foreign Influence	An individual may be subject to divided loyalties, manipulation, or coercion due to foreign associations or financial interests.
Guideline C	Foreign Preference	An individual who prefers a foreign country over the U.S. may make decisions that are harmful to the interests of national security.

Term	Definition/Explanation	Concern
Guideline D	Sexual Behavior	Some sexual behavior can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information, or, make the individual susceptible to blackmail.
Guideline E	Personal Conduct	Behavior that demonstrates questionable judgment, dishonesty, or an unwillingness to comply with rules and regulations, and could indicate that an individual will not properly safeguard classified information.
Guideline F	Financial Considerations	Indebtedness or irresponsible financial behavior indicates unreliability and may also provide motivation for espionage.
Guideline G	Alcohol Consumption	Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, and failure to control impulses.
Guideline H	Drug Involvement	Drug involvement raises questions about an individual's reliability and trustworthiness, both because drug use may impair judgment, and because it raises questions about an individual's willingness to comply with laws, rules, and regulations.
Guideline I	Psychological Conditions	Emotional, mental, and personality conditions may impair judgment, reliability, or trustworthiness.
Guideline J	Criminal Conduct	Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness and calls into question a person's ability or willingness to comply with laws, rules, and regulations.
Guideline K	Handling Protected Information	Failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information.

Term	Definition/Explanation	Concern
Guideline L	Outside Activities	Certain types of outside employment or activities may pose a conflict of interest with an individual's security responsibilities.
Guideline M	Use of Information Technology Systems	Failure to comply with the regulations governing IT systems raises serious concerns about an individual's reliability and trustworthiness.

Roles of DoD CAF in Adjudications

What about Brenda and her application for eligibility? Let's see how it's going. OPM, the ISP conducting Brenda's investigation, has completed its investigation and forwarded the results to the DoD CAF to evaluate Brenda's application and make an adjudicative determination. The adjudicator at the DoD CAF reviewed and evaluated the investigation results. By applying the thirteen adjudicative guidelines using the whole person concept, the adjudicator decided that granting Brenda eligibility to access classified information would be consistent with national security. If the DoD CAF makes an unfavorable adjudicative determination, then the applicant may appeal the determination to the Defense Office of Hearings and Appeals (DOHA).

Applicant Notification

Once an eligibility determination has been made, how is the applicant notified? Regardless of whether the adjudicative determination granted or denied eligibility, the decision is recorded in the DoD system of record and the applicant's FSO is notified via the DoD system of record. The FSO, in turn, notifies the applicant.

Review Activity

Review Activity 1

What is the order of steps in initiating the personnel security clearance request process?

Select where each task occurs in initiating the personnel security clearance request process. Check your answers in the Answer Key at the end of this Student Guide.

1 of 6: Step 1

- ○ Complete SF-86.
- ○ Submit fingerprint card.

- FSO reviews security clearance package.
- Check for pre-existing eligibility.
- Submit security clearance package.
- Initiate PCL request.

2 of 6: Step 2

- Complete SF-86.
- Submit fingerprint card.
- FSO reviews security clearance package.
- Check for pre-existing eligibility.
- Submit security clearance package.
- Initiate PCL request.

3 of 6: Step 3

- Complete SF-86.
- Submit fingerprint card.
- FSO reviews security clearance package.
- Check for pre-existing eligibility.
- Submit security clearance package.
- Initiate PCL request.

4 of 6: Step 4

- Complete SF-86.
- Submit fingerprint card.
- FSO reviews security clearance package.
- Check for pre-existing eligibility.
- Submit security clearance package.
- Initiate PCL request.

5 of 6: Step 5

- Complete SF-86.
- Submit fingerprint card.
- FSO reviews security clearance package.
- Check for pre-existing eligibility.

- ○ Submit security clearance package.
- ○ Initiate PCL request.

6 of 6: Step 6

- ○ Complete SF-86.
- ○ Submit fingerprint card.
- ○ FSO reviews security clearance package.
- ○ Check for pre-existing eligibility.
- ○ Submit security clearance package.
- ○ Initiate PCL request.

Review Activity 2

Who is responsible for each of the following activities during the PCL process?

Select FSO, PSMO-I, OPM, DoD CAF or DOHA for each activity. Check your answer in the Answer Key at the end of this Student Guide.

1 of 5: Initiates the PCL request.

- ○ FSO
- ○ PSMO-I
- ○ OPM
- ○ DoD CAF
- ○ DOHA

2 of 5: Performs an interim review of the submitted security clearance package.

- ○ FSO
- ○ PSMO-I
- ○ OPM
- ○ DoD CAF
- ○ DOHA

3 of 5: Performs a personnel security investigation on the applicant.

- ○ FSO
- ○ PSMO-I
- ○ OPM

- ○ DoD CAF
- ○ DOHA

4 of 5: Makes the adjudicative determination.

- ○ FSO
- ○ PSMO-I
- ○ OPM
- ○ DoD CAF
- ○ DOHA

5 of 5: Handles an applicant's appeal of an unfavorable adjudication.

- ○ FSO
- ○ PSMO-I
- ○ OPM
- ○ DoD CAF
- ○ DOHA

Review Activity 3

Who is responsible for each of the following activities during the PCL process?

Select FSO, PSMO-I, OPM, DoD CAF or DOHA for each activity. Check your answer in the Answer Key at the end of this Student Guide.

1 of 4: Which of the following is reviewed by the FSO to determine if a candidate has a pre-existing eligibility determination?

- ○ DoD System of Record
- ○ e-QIP

2 of 4: Which of the following is used to initiate a PCL Request?

- ○ DoD System of Record
- ○ e-QIP

3 of 4: Which of the following is used to complete the SF-86?

- ○ DoD System of Record
- ○ e-QIP

4 of 4: Which of the following is used by the FSO to review and submit an applicant's SF-86?

- ○ DoD System of Record
- ○ e-QIP

Review Activity 4

Match each type of background investigation to its correct access requirement.

For each access requirement, select Tier 3, Tier 5, Tier 3R or Tier 5R. Check your answer in the Answer Key at the end of this Student Guide.

1 of 4: An individual requires an initial investigation for Top Secret eligibility

- ○ Tier 3
- ○ Tier 5
- ○ Tier 3R
- ○ Tier 5R

2 of 4: An individual requires an updated investigation for Top Secret eligibility

- ○ Tier 3
- ○ Tier 5
- ○ Tier 3R
- ○ Tier 5R

3 of 4: An individual requires an initial investigation for Secret or Confidential eligibility

- ○ Tier 3
- ○ Tier 5
- ○ Tier 3R
- ○ Tier 5R

4 of 4: An individual requires an updated investigation for Secret or Confidential eligibility

- ○ Tier 3
- ○ Tier 5
- ○ Tier 3R
- ○ Tier 5R

Review Activity 5

What do you know about how a subject's application is adjudicated?

For each question, select the best answer. Check your answer in the Answer Key at the end of this Student Guide.

1 of 2: Which of the following assesses both favorable and unfavorable information from both an applicant's past and the present?

- ○ Whole Person Concept
- ○ 13 Adjudicative Guidelines

2 of 2: Which of the following ensures all applicants are assessed using the same standardized criteria?

- ○ Whole Person Concept
- ○ 13 Adjudicative Guidelines

Lesson 4: Managing the PSP at a Cleared Facility

Lesson Introduction

Objectives

Managing the Personnel Security Program (PSP) at a cleared facility involves more than obtaining personnel security clearances (PCLs). Cleared employees must receive required security briefings at specified intervals and continuous evaluation must be implemented.

In this lesson, you will learn the key elements of managing a PSP at a cleared facility.

Here is the lesson objective:

- Identify key elements of the management of the personnel security program at a cleared facility

Obtaining Access to Classified Information

As you know, a PCL doesn't automatically grant the recipient access to classified information. Remember, eligibility does not equal access. A PCL and a need-to-know are required in order to have access to classified information. Recall that in order for an individual to possess a PCL, the FSO at the contractor facility must determine that access to classified information will be needed for the individual to perform his or her duties and the individual must receive a favorable eligibility determination. Although a PCL grants an individual eligibility, before being permitted access to classified information, contractor personnel must have a legitimate need-to-know, sign an SF-312, or Classified Information Nondisclosure Agreement, promising that they will not disclose classified information to unauthorized individuals, and must first complete all required security training.

Once an individual has obtained access to classified information, in order to maintain that access, the facility security officer (FSO) must engage in several continuous evaluation activities. These activities include periodic reinvestigations, reporting required information, and maintaining the accuracy of their employees' access records.

Personnel Security Briefings

Security Briefings Overview

Brenda's personnel security clearance (PCL) request has been processed and adjudicated. While it may appear that the PCL process ends when the applicant receives a favorable eligibility determination, there is actually more involved. As you just learned, although Brenda has eligibility, one of the other requirements she must meet in order to possess a PCL and obtain access to classified information, is to receive the appropriate security training.

Security Training

Personnel security training ensures that cleared individuals are aware of their rights and responsibilities regarding the handling and protection of classified materials. FSOs are responsible for providing both initial security briefings and refresher training to the cleared personnel employed at their facility.

An initial security briefing is provided to individuals who have received a favorable personnel security determination for the first time, and is required to be completed prior to granting the individual access. This training includes a threat awareness briefing, a counterintelligence (CI) awareness briefing, an overview of the security classification system, a discussion of employee reporting obligations and requirements, cybersecurity training, and a discussion of the security procedures and duties applicable to an employee's position in the company.

Once cleared individuals have received their initial security briefing and held a clearance for one year, they must receive refresher training at least annually. Refresher security training reinforces the information provided in the initial security training and informs cleared employees of changes in security regulations and policies.

How Facility Clearances Affect Personnel Clearances

Limiting Access

Recall that in order to access classified materials, a cleared individual must work at a cleared facility. Facility security clearances and personnel security clearances each have an impact on the other. As with personnel security clearances, in order to obtain a facility security clearance (FCL), the facility must require access to classified information, and this requirement must be verified. If the highest level of classified access required by any of Belacort's classified contracts is Secret, then Belacort's FCL will be issued at the Secret level and no higher. This means that any employee who receives an initial eligibility determination while working for Belacort will only ever receive it at the Secret level, since there is no requirement to access information classified at a higher level. But what about employees that Belacort hires who already hold a PCL? A cleared employee's access is limited by their facility's clearance level. This means that even if an employee has a pre-existing Top Secret PCL, if the facility's FCL is only to the Secret level, then the employee may only access information classified at the Secret level while employed with that contractor.

The Facility Clearance Process

A contractor who has been awarded a classified contract will require an FCL in order to access classified information at its facility. Receiving an FCL is contingent upon all of the required key management personnel (KMP) either receiving PCLs, or completing exclusion resolutions. KMP, such as senior management officials, the Insider Threat Program Senior Official (ITPSO), and the FSO, must be cleared to the same level as the FCL before a final FCL will be granted. Employees and other KMPs that require classified access may be processed for a PCL concurrently with the FCL request, if immediate access is required, or after the FCL has been granted. KMP's not required to be cleared in

connection with the FCL, may be formally excluded from access by executing the associated exclusion resolution. For more information on the facility security clearance process see the Facility Clearances in the NISP course.

Continuous Evaluation

Overview

Recall that only individuals who possess a PCL and have a legitimate need-to-know may access classified information. Once access has been obtained, the FSO is responsible for helping cleared employees maintain their ability to access classified information by implementing a continuous evaluation program. Under continuous evaluation (CE), FSOs must initiate periodic reinvestigations and report required information appropriately. However, in the near future, an automated records check monitoring system will become an integral part of CE, and cover the gap between initial investigation and the periodic reinvestigation. FSOs are also required to maintain the accuracy of their employee access records. We will examine each of these elements of continuous evaluation.

Periodic Reinvestigations

Eligibility determinations do not expire, even if the subject is overdue for a periodic reinvestigation. While an individual may have received a favorable initial eligibility determination, in order to be allowed continued access to classified information, that eligibility determination must be periodically updated so that it is based on a current investigation. An individual with a Top Secret, Secret, or Confidential eligibility determination must undergo a reinvestigation every 5 years. As you learned previously, this is a change for Secret and Confidential eligibility determinations per the new Federal Investigative Standards. However, per the FIS implementation guidance, 10 year reinvestigation intervals are permitted for continued eligibility and access for Secret information until full operating capability of Tier 3, which is anticipated by October 2017.

While PSMO-I may notify the FSO when KMP are eligible for a periodic reinvestigation, for all other cleared employees, the FSO must run a periodic reinvestigation report in the DoD system of record to determine who is eligible or overdue for a periodic reinvestigation. The FSO then reviews access records to ensure that the prospective subject of a periodic reinvestigation still requires access to classified information. If the individual does still require access, then the FSO will submit a periodic reinvestigation request. If the individual does not still require access, then no periodic reinvestigation is required.

Reporting Required Information

To maintain current information on cleared individuals, FSOs must report required information appropriately. The National Industrial Security Program Operating Manual (NISPOM) provides the requirements for reporting. In general, FSOs must report events or information that have an impact on the status of the facility security clearance (FCL) that affect the status of an employee's personnel security clearance, may indicate the employee poses an insider threat, that affect proper

safeguarding of classified information, or that indicate that classified information has been lost or compromised. For more information on the contractor's requirements to report certain information, see the NISP Reporting Requirements course.

PCL Reporting Requirements

Information that may affect an individual's PCL is reported directly to PSMO-I. FSOs are required to report adverse information concerning a cleared employee, any suspicious contacts, a cleared employee not wishing to perform work on a classified project, or a cleared employee refusing to sign the Classified Information Nondisclosure Agreement (SF-312). Any change in the status of a cleared employee such as death, name change, change in citizenship, termination of employment, or being barred from future access to classified information must also be reported. And finally, reports about employee involvement in the loss, compromise, or suspected compromise of classified material must also be reported to PSMO-I.

Maintaining Employee Access Records

The NISPOM requires contractors to maintain the accuracy of their employees' access records. One way that many FSOs meet this requirement is by conducting an annual clearance justification review to ensure that their facility's cleared employees still have a valid requirement to access classified information. One method for conducting an annual clearance review is distributing an electronic questionnaire to facility personnel asking basic PCL questions. Note that annual clearance justification reviews are just one way to meet the NISPOM's requirement and are considered a best practice, but they are not required security policy. In addition to clearance justification reviews, when notified of the denial, revocation or suspension of an employee's PCL, FSOs are required to immediately deny that employee access to classified information.

Review Activity

Review Activity 1

What do you know about PSP activities after the PCL process has been completed?

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

1 of 3: Once applicants receive a favorable eligibility determination, they may access classified information immediately.

- ○ True
- ○ False

2 of 3: Eligibility determinations expire after a certain number of years depending on their classification level.

- ○ True
- ○ False

3 of 3: Annual clearance justification reviews to ensure cleared employees still require access to classified information are required by security policy.

- ○ True
- ○ False

Review Activity 2

What do you know about periodic reinvestigations?

For each question, select the best answer. Check your answers in the Answer Key at the end of this Student Guide.

1 of 3: An individual with Confidential eligibility must undergo a reinvestigation every_____.

- ○ 5 years
- ○ 10 years
- ○ 15 years

2 of 3: An individual with Top Secret eligibility must undergo a reinvestigation every_____.

- ○ 5 years
- ○ 10 years
- ○ 15 years

3 of 3: An individual with Secret eligibility must undergo a reinvestigation every 5 years but it can be every _____ years until full implementation of Tier 3.

- ○ 5 years
- ○ 10 years
- ○ 15 years

Review Activity 3

In general, FSOs are required to report events or information that do which of the following?

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

- ☐ Affect the status of the FCL
- ☐ Affect the status of an employee's PCL
- ☐ Affect proper safeguarding of classified information
- ☐ Indicate classified information has been lost/compromised
- ☐ Indicate the employee poses an insider threat

Lesson 5: Personnel Clearances Challenge

Lesson Introduction

Getting Started

Welcome to the Personnel Clearances Challenge. This challenge will give you a chance to practice identifying what is required in the Personnel Security Program (PSP) at cleared facilities. Here's how it works. As the Facility Security Officer (FSO), you'll make decisions regarding the management of the PSP. You will select items in your office, such as file folders and email messages. When you select each one, you'll see a question related to the PSP. In the Answer Key at the end of this Student Guide, you will receive feedback which may include some additional information about that item.

Personnel Security Clearances

Email Notification: Classified Contract Award

You just received an e-mail about a contract award.

To: The Team
From: Jonathan Baker
Subject: Contract Award

Hello Team,

We are happy to let you know we won the contract you all worked so hard on. We appreciate the late nights you spent helping with the proposal. This is a 5-year contract and is classified as SECRET. Everyone who works on this contract must have at least a SECRET clearance. Our FSO will begin working on this now.

Thanks,

Jonathan Baker
Director, Business Development Team

Question 1

The Federal Investigative Standards are fully implemented, you check the DoD system of record to determine the eligibility status of each cleared employee who will be working on this new SECRET contract. You see that Brian, the instructional designer, obtained his SECRET clearance over 5 years ago and Diane, the digital artist, obtained her SECRET clearance almost 10 years ago. For whom do you need to initiate a periodic reinvestigation?

Determine which answer is correct. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Diane requires a periodic reinvestigation, but Brian does not since SECRET reinvestigations are required every 10 years.
- ○ Neither Brian nor Diane requires a periodic reinvestigation at this time since SECRET reinvestigations are required every 15 years.
- ○ Both Brian and Diane require a periodic reinvestigation at this time since SECRET reinvestigations are required every 5 years.

Question 2

Your company recently hired a new programmer, Lindsay. She is slated to work on the new SECRET contract, but to your knowledge, Lindsay does not yet have a personnel security clearance. As the FSO, what do you need to do before Lindsay completes the Questionnaire for National Security Positions (SF-86) in eQIP?

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

- ☐ Verify that Lindsay is a U.S. citizen
- ☐ Perform any necessary agency checks
- ☐ Review DoD system of record (JPAS or DISS) to see if Lindsay has a pre-existing record
- ☐ Initiate PCL request

Continuous Evaluation

Folder: Information about Employee

Now select the blank manila folder someone left on your desk to see what's in it. Looks like Lindsay does not want to sign the SF-312 even though you just received notification that her eligibility was granted. She left you a note stating, "I do not feel comfortable signing the SF-312, so I will not sign it. I am requesting not to work on the classified contract. Thank you, Lindsay Smith"

Question 1

After speaking with Lindsay in person, she confirms that she really does not want to sign the SF-312. What should you do?

Determine which answer is correct. Check your answer in the Answer Key at the end of this Student Guide.

- ○ You should submit an Adverse Information Report about Lindsay for not signing the SF-312.
- ○ You should not report Lindsay for not signing the SF-312 but simply move her to a non-classified contract.

- ○ You should not report Lindsay for not signing the SF-312 but recommend that she be fired.

Question 2

To whom should you submit the Adverse Information Report about Lindsay refusing to sign the SF-312?

Determine which answer is correct. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Federal Bureau of Investigation (FBI)
- ○ Personnel Security Management Office for Industry (PSMO-I)
- ○ Office of Personnel Management (OPM)

Facility Clearances

Email Notification: Promotion

You just received another e-mail. Looks like a new President has been selected for your company.

To: The Team
From: Suzy Johannes
Subject: New President

Hello Team,

I am pleased to announce Julie Green was recently selected to be your new company President. Please join me in welcoming Julie!

Thanks,

Suzy Johannes
Owner

Question 1

Julie Green has been selected as the new President of your company. Will you need to initiate the personnel security clearance process for Julie?

Determine which answer is correct. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Yes, Julie will need a PCL since she will hold a key management personnel (KMP) position that is required to be cleared in connection with the facility clearance.

- ○ No, Julie's position is not one that requires her to be cleared in connection with the facility clearance, but you will need to execute an exclusion resolution and place her on your KMP list.
- ○ No, Julie does not need a PCL since she will not be working directly on the classified contract.

Security Education and Training

Folder: Security Education and Training

Now select the folder labeled Security Education and Training. There are two documents inside the folder labeled Initial Security Briefing and Refresher Security Training, Once all of the employees who will be working on the classified contract have received their personnel security clearances, you must ensure they are aware of their rights and responsibilities regarding the handling and protection of classified materials.

Question 1: Initial Security Briefing

When you put together the initial security briefing for the employees with new personnel security clearances, what information are you required to include?

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

- ☐ Security procedures and duties applicable to an employee's position
- ☐ Employee reporting requirements
- ☐ CI Awareness briefing
- ☐ Threat awareness briefing
- ☐ Overview of security classification system
- ☐ Cybersecurity training

Lesson 6: Course Conclusion

Course Conclusion

Course Summary

Personnel security clearances (PCLs) as part of the personnel security program (PSP) ensure that only loyal, trustworthy, and reliable individuals are allowed to access classified information, thereby helping to protect our national security. The process to obtain a PCL involves obtaining detailed information about the applicant, conducting an investigation of the applicant, and evaluating the results of that investigation to make an adjudicative determination. The contractor's responsibility under the PSP does not end with the issuance of a favorable eligibility determination, however. Maintaining a PCL and managing the PSP program at a cleared contractor facility involves a variety of continuous evaluation activities.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- Overview of Personnel Clearances in the NISP
- Processing PCL Eligibility
- Managing the PSP at a Cleared Facility
- Personnel Clearances Challenge
- Course Conclusion

Course Objectives

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

- Identify the legal and regulatory basis of the personnel security program
- Identify key terms relating to personnel security
- Identify the role of various organizational components (PSMO-I, DoD CAF, DOHA) in the NISP personnel security clearance process for industry contractors
- Identify contractor, applicant, and government responsibilities in the processing of personnel security clearance eligibility
- Identify the basic and common functions of the DoD system of record, including the system's use of the terms "eligibility" and "access"

- Identify the revised Federal Investigative Standards (FIS) used to make national security eligibility determinations
- Identify the adjudicative standards for the personnel security program
- Identify key elements of the management of the personnel security program at a cleared facility

Congratulations. You have completed the Personnel Clearances in the NISP course. To receive course credit, you MUST take the Personnel Clearances in the NISP examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.

Appendix A: Answer Key—Review Activities

Lesson 2 Review Activities (Answer Key)

Review Activity 1

For each question, select the best answer.

1 of 4: _____ is vested with worldwide responsibility under the National Industrial Security Program (NISP) for processing and tracking applications for industrial personnel security clearances.

- ○ DoD CAF
- ⦿ PSMO- I (correct response)

***Feedback**: PSMO-I has worldwide responsibility under the NISP for processing and tracking applications for industrial personnel security clearances, and performs as the Cognizant Government Authority for personnel security management and oversight under the NISP.*

2 of 4: _____ typically determines personnel security clearance eligibility of contractor employees.

- ⦿ DoD CAF (correct response)
- ○ DOHA

***Feedback**: DoD CAF determines the personnel security clearance eligibility of contractor employees supporting the DoD and 31 other agencies in most cases.*

3 of 4: _____ processes and tracks applications for industrial personnel security clearances, and performs as the Cognizant Government Authority for personnel security management and oversight under the NISP.

- ⦿ PSMO- I (correct response)
- ○ DOHA

***Feedback**: PSMO-I processes and tracks applications for industrial personnel security clearances, and performs as the Cognizant Government Authority for personnel security management and oversight under the NISP.*

4 of 4: _____ decides unfavorable eligibility determinations that are appealed.

- ○ DoD CAF
- ⦿ DOHA (correct response)

***Feedback**: DOHA provides hearings and issues decisions in eligibility cases that involve attempts to appeal an unfavorable eligibility determination.*

Review Activity 2

Indicate who uses each system or secure website for each statement.

1 of 3: Retrieves DoD PCL eligibility information in the DoD system of record

- ⦿ FSO (correct response)
- ○ Contractor Employee

2 of 3: Initiates PCL investigation requests from the DoD system of record

- ⦿ FSO (correct response)
- ○ Contractor Employee

3 of 3: Completes the Questionnaire for National Security Positions using e-QIP

- ○ FSO
- ⦿ Contractor Employee (correct response)

Review Activity 3

Indicate which regulation or resource matches each description.

1 of 3: Used in the PCL process to help in determining a candidate's eligibility

- ○ E.O. 12968
- ○ NISPOM
- ◉ Adjudicative Guidelines (correct response)

2 of 3: Provides policy about PCLs and defines the requirements for accessing classified information

- ◉ E.O. 12968 (correct response)
- ○ NISPOM
- ○ Adjudicative Guidelines

3 of 3: Provides requirements regarding PCLs among other aspects of the NISP

- ○ E.O. 12968
- ◉ NISPOM (correct response)
- ○ Adjudicative Guidelines

Lesson 3 Review Activities (Answer Key)

Review Activity 1

What is the order of steps in initiating the personnel security clearance request process?

Select where each task occurs in initiating the personnel security clearance request process.

1 of 6: Step 1

- ○ Complete SF-86.
- ○ Submit fingerprint card.
- ○ FSO reviews security clearance package.
- ◉ Check for pre-existing eligibility. (correct response)
- ○ Submit security clearance package.
- ○ Initiate PCL request.

2 of 6: Step 2

- ○ Complete SF-86.
- ○ Submit fingerprint card.
- ○ FSO reviews security clearance package.
- ○ Check for pre-existing eligibility.
- ○ Submit security clearance package.
- ◉ Initiate PCL request. (correct response)

3 of 6: Step 3

- ◉ Complete SF-86. (correct response)
- ○ Submit fingerprint card.

- ○ FSO reviews security clearance package.
- ○ Check for pre-existing eligibility.
- ○ Submit security clearance package.
- ○ Initiate PCL request.

4 of 6: Step 4

- ○ Complete SF-86.
- ○ Submit fingerprint card.
- ◉ FSO reviews security clearance package. (correct response)
- ○ Check for pre-existing eligibility.
- ○ Submit security clearance package.
- ○ Initiate PCL request.

5 of 6: Step 5

- ○ Complete SF-86.
- ○ Submit fingerprint card.
- ○ FSO reviews security clearance package.
- ○ Check for pre-existing eligibility.
- ◉ Submit security clearance package. (correct response)
- ○ Initiate PCL request.

6 of 6: Step 6

- ○ Complete SF-86.
- ◉ Submit fingerprint card. (correct response)
- ○ FSO reviews security clearance package.

- ○ Check for pre-existing eligibility.
- ○ Submit security clearance package.
- ○ Initiate PCL request.

Review Activity 2

Who is responsible for each of the following activities during the PCL process?

Select FSO, PSMO-I, OPM, DoD CAF or DOHA for each activity.

1 of 5: Initiates the PCL request.

- ⦿ FSO (correct response)
- ○ PSMO-I
- ○ OPM
- ○ DoD CAF
- ○ DOHA

***Feedback**: The FSO uses the DoD system of record to initiate the PCL Request.*

2 of 5: Performs an interim review of the submitted security clearance package.

- ○ FSO
- ⦿ PSMO-I (correct response)
- ○ OPM
- ○ DoD CAF
- ○ DOHA

***Feedback**: PSMO-I conducts a review of the submitted security clearance package to determine if interim eligibility will be granted to the applicant.*

3 of 5: Performs a personnel security investigation on the applicant.

- ○ FSO
- ○ PSMO-I
- ◉ OPM (correct response)
- ○ DoD CAF
- ○ DOHA

***Feedback**: OPM is the investigative provider that conducts the appropriate background investigation of the applicant.*

4 of 5: Makes the adjudicative determination.

- ○ FSO
- ○ PSMO-I
- ○ OPM
- ◉ DoD CAF (correct response)
- ○ DOHA

***Feedback**: After evaluating the investigation results, DoD CAF determines whether the applicant is eligible for access.*

5 of 5: Handles an applicant's appeal of an unfavorable adjudication.

- ○ FSO
- ○ PSMO-I
- ○ OPM
- ○ DoD CAF
- ◉ DOHA (correct response)

***Feedback**: DOHA processes appeals when an applicant contests an unfavorable determination by DoD CAF.*

Review Activity 3

Who is responsible for each of the following activities during the PCL process?

Select FSO, PSMO-I, OPM, DoD CAF or DOHA for each activity.

1 of 4: Which of the following is reviewed by the FSO to determine if a candidate has a pre-existing eligibility determination?

- ⦿ DoD System of Record (correct response)
- ○ e-QIP

Feedback: *The FSO reviews the DoD system of record to determine if the applicant has a record in that system, if the applicant has a pre-existing favorable eligibility determination, and if any pre-existing determination may be accepted in lieu of initiating a new investigation and adjudication process.*

2 of 4: Which of the following is used to initiate a PCL Request?

- ⦿ DoD System of Record (correct response)
- ○ e-QIP

Feedback: *The FSO uses the DoD system of record to initiate a PCL Request.*

3 of 4: Which of the following is used to complete the SF-86?

- ○ DoD System of Record
- ⦿ e-QIP (correct response)

Feedback: *The applicant uses e-QIP to complete the SF-86.*

4 of 4: Which of the following is used by the FSO to review and submit an applicant's SF-86?

- ○ DoD System of Record
- ⦿ e-QIP (correct response)

Feedback: *The FSO uses e-QIP to review the applicant's SF-86 to ensure it is adequate and complete and then to submit the completed SF-86.*

Review Activity 4

Match each type of background investigation to its correct access requirement.

For each access requirement, select Tier 3, Tier 5, Tier 3R or Tier 5R.

1 of 4: An individual requires an initial investigation for Top Secret eligibility

- ○ Tier 3
- ◉ Tier 5 (correct response)
- ○ Tier 3R
- ○ Tier 5R

2 of 4: An individual requires an updated investigation for Top Secret eligibility

- ○ Tier 3
- ○ Tier 5
- ○ Tier 3R
- ◉ Tier 5R (correct response)

3 of 4: An individual requires an initial investigation for Secret or Confidential eligibility

- ◉ Tier 3 (correct response)
- ○ Tier 5
- ○ Tier 3R
- ○ Tier 5R

4 of 4: An individual requires an updated investigation for Secret or Confidential eligibility

- ○ Tier 3
- ○ Tier 5
- ⦿ Tier 3R (correct response)
- ○ Tier 5R

Review Activity 5

What do you know about how a subject's application is adjudicated?

For each question, select the best answer.

1 of 2: Which of the following assesses both favorable and unfavorable information from both an applicant's past and the present?

- ⦿ Whole Person Concept (correct response)
- ○ 13 Adjudicative Guidelines

Feedback: *To conduct a review that is fair and free of bias, adjudicators apply the Whole Person Concept, which assesses both unfavorable and favorable information about an individual, drawing such information from both the individual's past and the present.*

2 of 2: Which of the following ensures all applicants are assessed using the same standardized criteria?

- ○ Whole Person Concept
- ⦿ 13 Adjudicative Guidelines (correct response)

Feedback: *To conduct a review that is fair and free of bias, adjudicators utilize 13 standardized adjudicative guidelines when evaluating the results of an applicant's personnel investigation.*

Lesson 4 Review Activities (Answer Key)

Review Activity 1

What do you know about PSP activities after the PCL process has been completed?

Select True or False for each statement.

1 of 3: Once applicants receive a favorable eligibility determination, they may access classified information immediately.

- ○ True
- ⦿ False (correct response)

Feedback: *Although an individual may be granted eligibility, an initial security briefing must be completed before access to classified information is allowed.*

2 of 3: Eligibility determinations expire after a certain number of years depending on their classification level.

- ○ True
- ⦿ False (correct response)

Feedback: *Eligibility determinations do not expire; however, in order for an individual who has a favorable eligibility determination to continue to have access to classified information, the eligibility determination must be based on a current personnel security investigation.*

3 of 3: Annual clearance justification reviews to ensure cleared employees still require access to classified information are required by security policy.

- ○ True
- ⦿ False (correct response)

Feedback: *Although not required by security policy, annual clearance justification reviews are a best practice.*

Review Activity 2

What do you know about periodic reinvestigations?

For each question, select the best answer.

1 of 3: An individual with Confidential eligibility must undergo a reinvestigation every_____.

- ⦿ 5 years (correct response)
- ○ 10 years
- ○ 15 years

Feedback: *Although eligibility determinations never expire, in order for individuals with a favorable eligibility determination for Confidential clearance to be allowed access to classified information, their eligibility determination must be based on a personnel security investigation that is current to within 5 years, per the new FIS.*

2 of 3: An individual with Top Secret eligibility must undergo a reinvestigation every_____.

- ⦿ 5 years (correct response)
- ○ 10 years
- ○ 15 years

Feedback: *Although eligibility determinations never expire, in order for individuals with a favorable eligibility determination for Top Secret clearance to be allowed access to classified information, their eligibility determination must be based on a personnel security investigation that is current to within 5 years.*

3 of 3: An individual with Secret eligibility must undergo a reinvestigation every 5 years but it can be every _____ years until full implementation of Tier 3.

- ○ 5 years
- ⦿ 10 years (correct response)
- ○ 15 years

Feedback: *Although eligibility determinations never expire, in order for individuals with a favorable eligibility determination for Secret clearance to be allowed access to classified information, their eligibility determination must be based on a personnel security investigation that is current to within 5 years, per the new FIS.*

Review Activity 3

In general, FSOs are required to report events or information that do which of the following?

Select all that apply.

- ☑ Affect the status of the FCL (correct response)
- ☑ Affect the status of an employee's PCL (correct response)
- ☑ Affect proper safeguarding of classified information (correct response)
- ☑ Indicate classified information has been lost/compromised (correct response)
- ☑ Indicate the employee poses an insider threat (correct response)

Feedback: *FSOs are required to report events or information that do any and all of these things.*

Lesson 5 Review Activities (Answer Key)

Question 1: Personnel Security Clearances

The Federal Investigative Standards are fully implemented, you check the DoD system of record to determine the eligibility status of each cleared employee who will be working on this new SECRET contract. You see that Brian, the instructional designer, obtained his SECRET clearance over 5 years ago and Diane, the digital artist, obtained her SECRET clearance almost 10 years ago. For whom do you need to initiate a periodic reinvestigation?

Determine which answer is correct.

- ○ Diane requires a periodic reinvestigation, but Brian does not since SECRET reinvestigations are required every 10 years.
- ○ Neither Brian nor Diane requires a periodic reinvestigation at this time since SECRET reinvestigations are required every 15 years.

⊙ Both Brian and Diane require a periodic reinvestigation at this time since SECRET reinvestigations are required every 5 years. (correct response)

Feedback: *The new 5 year reinvestigation requirement applies to TOP SECRET, SECRET and CONFIDENTIAL eligibility. While the new 5 year reinvestigation requirement is not a change for continuing Top Secret eligibility, it does replace the old investigative requirement of having a periodic reinvestigation every 10 years for continuing Secret eligibility and every 15 years for continuing Confidential eligibility.*

Question 2: Personnel Security Clearances

Your company recently hired a new programmer, Lindsay. She is slated to work on the new SECRET contract, but to your knowledge, Lindsay does not yet have a personnel security clearance. As the FSO, what do you need to do before Lindsay completes the Questionnaire for National Security Positions (SF-86) in eQIP?

Select all that apply.

☑ Verify that Lindsay is a U.S. citizen (correct response)

☐ Perform any necessary agency checks

☑ Review DoD system of record (JPAS or DISS) to see if Lindsay has a pre-existing record (correct response)

☑ Initiate PCL request (correct response)

Feedback: *You will need to verify Lindsay is a U.S. citizen by examining her birth certificate, passport or any of the other documents listed in the NISPOM. Remember, forms of identification accepted as part of the I-9 Employment Eligibility Verification Form are not sufficient for this purpose. You will also need to review the DoD system of record to see if Lindsay has a pre-existing record and, if she does, if she has a pre-existing eligibility determination. Then you will need to assess whether the determination may be accepted in lieu of a new investigation or if a new investigation is required. Next you will need to initiate Lindsay's PCL request using the DoD system of record.*

Question 1: Continuous Evaluation

After speaking with Lindsay in person, she confirms that she really does not want to sign the SF-312. What should you do?

Determine which answer is correct.

⊙ You should submit an Adverse Information Report about Lindsay for not signing the SF-312. (correct response)

- ○ You should not report Lindsay for not signing the SF-312 but simply move her to a non-classified contract.
- ○ You should not report Lindsay for not signing the SF-312 but recommend that she be fired.

Feedback: *You should submit an Adverse Action Report. FSOs are required to report a cleared employee not wishing to perform on a classified project or a cleared employee refusing to sign the Classified Information Nondisclosure Agreement (SF-312).*

Question 2: Continuous Evaluation

To whom should you submit the Adverse Information Report about Lindsay refusing to sign the SF-312?

Determine which answer is correct.

- ○ Federal Bureau of Investigation (FBI)
- ⦿ Personnel Security Management Office for Industry (PSMO-I) (correct response)
- ○ Office of Personnel Management (OPM)

Feedback: *You will need to submit the report to PSMO-I.*

Question 1: Facility Clearances

Julie Green has been selected as the new President of your company. Will you need to initiate the personnel security clearance process for Julie?

Determine which answer is correct.

- ⦿ Yes, Julie will need a PCL since she will hold a key management personnel (KMP) position that is required to be cleared in connection with the facility clearance. (correct response)
- ○ No, Julie's position is not one that requires her to be cleared in connection with the facility clearance, but you will need to execute an exclusion resolution and place her on your KMP list.
- ○ No, Julie does not need a PCL since she will not be working directly on the classified contract.

Feedback: *Julie does need to obtain a PCL equivalent to that of your company's FCL as she is now a KMP of the company.*

Question 1: Initial Security Briefing

When you put together the initial security briefing for the employees with new personnel security clearances, what information are you required to include?

Select all that apply.

- ☑ Security procedures and duties applicable to an employee's position (correct answer)
- ☑ Employee reporting requirements (correct response)
- ☑ CI Awareness briefing (correct response)
- ☑ Threat awareness briefing (correct response)
- ☑ Overview of security classification system (correct response)
- ☑ Cybersecurity training (correct response)

Feedback: *You are required to include all of these items in your initial security briefing.*