Personnel Clearances in the National Industrial Security Program (NISP), Version 5

Student Guide

November 2024

Center for Development of Security Excellence

Personnel Clearances in the NISP

Table of Contents

Lesson 1: Course Introduction

Course Introduction

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	• DCSA Industrial Security Specialists • Facility Security Officers • Other security practitioners in the NISP
Pass %/Fail	75% on final examinations
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 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 PSP. As an important part of the PSP, this course will also discuss the process to obtain a favorable national security eligibility determination, also referred to as 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 roles of various government components in the NISP Personnel Security Clearance process for contractors
- Identify entity and individual responsibilities in the eligibility processing of Personnel Security Clearances
- Identify the basic and common functions of the DOD Personnel Security System of Record

- Identify the investigative model used to make national security eligibility determinations and the Continuous Vetting process
- Identify the national security adjudicative guidelines for the Personnel Security Program
- Identify Personnel Security Program key managing elements 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
- Personnel Clearances Challenge
- Course Conclusion

Lesson 2: Overview of Personnel Clearances in the NISP

Lesson Objectives

In order for the government to entrust individuals with classified information, the government must ensure those individuals are loyal, trustworthy, and reliable. When such individuals are working for a cleared contractor, 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 PSPs and PCLs. You will examine the roles of important government 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 government components in the NISP Personnel Security Clearance process for contractors
- Identify the legal and regulatory basis of the Personnel Security Program

Introduction to the NISP

The PSP protects national security by ensuring 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 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 in accordance with the 32 Code of Federal Regulation (CFR) Part 117, National Industrial Security Program Operating Manual, or (NISPOM), and related federal requirements for classified information.

Eligibility and Access

Before contractor personnel may access classified information, they must be granted a favorable national security eligibility determination, or PCL, to ensure access to classified information is in the best interest of national security. Once the contractor has determined and verified that access to classified information is essential in performance of tasks or services to the fulfillment of a classified contract, the FSO will initiate the employee's clearance process. Contractors will not submit requests for determination of eligibility for access to classified information for individuals who are not their employees, nor will they submit requests for employees of subcontractors. The employee will undergo the appropriate national security background investigation before a trained government adjudicator reviews and considers the results of the background investigation

in accordance with national security adjudicative guidelines. The adjudicator will then reach an eligibility determination on whether granting the individual access to classified information would be consistent with the national security interest of the United States.

It is important to note, however, that just because an individual is granted eligibility, it does not mean an individual may have access to classified information. To access classified information, an individual must have eligibility for access to classified information at the appropriate level and have a valid need-to-know for the 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. A Classified Information Nondisclosure Agreement (SF 312) must also be signed, and the NISPOM requires employees to receive an initial security briefing prior to being granted access to classified information.

The PSP in the NISP

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

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 look at the government components in the NISP PCL process for contractors.

Government Components

There are many entities involved in the NISP; however, a few government components are particularly relevant in determining an employee's eligibility for access to classified information.

Cognizant Security Agencies (CSAs) are agencies of the Executive Branch that have been authorized to establish industrial security programs to safeguard classified information within the NISP. The Department of Defense (DOD) is one of the CSAs, and it represents many other federal agencies and departments in this capacity. A Cognizant Security Office (CSO) is delegated by the head of the CSA to administer industrial security on behalf of the CSA.

The Defense Counterintelligence and Security Agency (DCSA) is the CSO for the DOD. Within DCSA, there are various components that work directly with personnel at contractor facilities. Divisions include duties that perform vetting, adjudications, and national security background investigations, along with the DCSA Field Offices where Industrial Security Representatives (IS Reps) work directly with their assigned contractor FSOs.

Other DOD organizations that may be involved in the eligibility determination process is the Defense Office of Hearings and Appeals (DOHA).

Contractor Components

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

The FSO oversees the implementation of the facility's security program and works directly with the government components involved in the NISP. In addition, Key Management Personnel (KMP) are company officials who either hold majority interest or stock in, or have direct or indirect authority to, influence or decide issues affecting the management or operations of classified contract performance. The KMP of a facility must include the Senior Management Official (SMO), the Facility Security Officer (FSO), and the Insider Threat Program Senior Official (ITPSO).

Note that to be approved as a cleared facility, a company must meet the specific requirements for a favorable entity eligibility determination, also referred to as a Facility Clearance (FCL). To obtain an FCL, essential KMP must be cleared to the same level or above the company FCL in addition to meeting other administrative requirements.

Communicating PCL Information

Now that you have learned about the government components involved in the NISP PCL process for contractors, let's look at how these different entities communicate with one another regarding PCLs. The DOD Personnel Security System of Record is the system that has connected FSOs and other security program managers with a single database for managing and maintaining PCL eligibility and access. It also allows the contractor to access and update PCL eligibility information, thereby ensuring reciprocity. If an individual does not have eligibility, then the contractor can initiate the clearance process to obtain an eligibility determination. Contractor employees must provide information about themselves by electronically completing the Questionnaire for National Security Positions, also referred to as the SF-86, and furnishing other documentation as well.

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 the NISPOM. This manual provides guidance to FSOs about how to implement security program policy and requirements for PCLs issued under the NISP.

Meet Brenda Taylor. She's a new hire at a cleared company called Belacort Industries. Brenda's project manager notifies Belacort's FSO, Ted Fuller, that Brenda will require access to classified information in performance of her duties. Mr. Fuller asks to meet with Brenda to discuss the PCL eligibility process.

Because this process is new to Brenda, she asks Mr. Fuller to explain the guidelines for deciding her eligibility determination. Mr. Fuller consults the National Security Adjudicative Guidelines and explains the criteria to Brenda. This is a key resource to have access to as an FSO administering a personnel security program for a cleared facility. FSOs are strongly encouraged to include the adjudicative guidelines in initial security briefings and refresher training, as appropriate.

Review Activity 1

For each question, select the best answer.

Question 1 of 4
_____ are agencies of the Executive Branch that have been authorized to establish industrial security programs to safeguard classified information within the NISP.

- o CSOs
- o CSAs

Answer: CSAs are agencies of the Executive Branch that have been authorized to establish industrial security programs to safeguard classified information within the NISP.

Question 2 of 4
_____ is delegated by the head of the CSA to administer industrial security on behalf of the CSA.

- o CSO
- o DOHA

Answer: A CSO is delegated by the head of the CSA to administer industrial security on behalf of the CSA.

Question 3 of 4

_____ are company officials who either hold majority interest or stock in or have direct or indirect authority to influence or decide issues affecting the management or operations of the company or classified contract performance.

- o KMP
- o IS REP

Answer: KMP are company officials who either hold majority interest or stock in or have direct or indirect authority to, influence or decide issues affecting the management or operations of the company or classified contract performance.

Question 4 of 4
_____ performs vetting, adjudications, and national security background investigations.

- o DCSA
- o DOHA

Answer: DCSA performs vetting, adjudications, and national security background investigations.

Review Activity 2

Indicate to whom each statement applies to.

Question 1 of 3
Manages and maintains PCL eligibility and access using the DOD Personnel Security System of Record

- o FSO
- o Contractor Employee

Answer: FSO

Question 2 of 3
Initiates the employee's clearance process in the DOD Personnel Security System of Record
- FSO
- Contractor Employee

Answer: FSO

Question 3 of 3
Completes the Questionnaire for National Security Positions
- FSO
- Contractor Employee

Answer: Contractor Employee

Review Activity 3

Indicate which regulation or resource matches each description.

Question 1 of 3
Provides policy about PCLs and defines the requirements for accessing classified information.
- E.O. 12968
- NISPOM
- National Security Adjudicative Guidelines

Answer: E.O. 12968

Question 2 of 3
Provides security program requirements about PCLs under the NISP.
- E.O. 12968
- NISPOM
- National Security Adjudicative Guidelines

Answer: NISPOM

Question 3 of 3
Criteria used in the PCL process to help determine a candidate's PCL eligibility determination.
- E.O. 12968
- NISPOM
- National Security Adjudicative Guidelines

Answer: National Security Adjudicative Guidelines

Lesson 3: Processing NISP PCL Eligibility

Lesson Objectives

The 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 the government in the NISP PCL process. You will identify the common functions of the DOD Personnel Security System of Record.

You will learn about the investigative model used to make PCL eligibility determinations and the process for Continuous Vetting.

You will also identify the national security adjudicative guidelines for the PSP.

Here are the lesson objectives:

- Identify entity and individual responsibilities in the eligibility processing of
- Identify the basic and common functions of the DOD Personnel Security System of Record
- Identify the investigative model used to make national security eligibility determinations and the Continuous Vetting process
- Identify the national security adjudicative guidelines for the Personnel Security Program

Processing a Request for a PCL

Requesting, processing, and receiving a PCL eligibility determination involves various stages. Once the determination is made and verified that an employee or prospective employee requires access to classified information to perform job-related duties, the contractor initiates the clearance request process via the DOD Personnel Security System of Record. Employees must provide information about themselves by electronically completing a Security Questionnaire. Then information is released to DCSA for vetting and interim clearance determination, pending completion of the full national security background investigation. Investigators from DCSA, or an Investigations Service Provider (ISP), will perform the appropriate background agency checks and conducts interviews when applicable. The investigation results are reviewed and adjudicated by DCSA in accordance with national security adjudicative guidelines to reach a final eligibility determination.

Overview of Initiation Activities

Initiating the PCL process involves several steps. First, the FSO verifies the employee's U.S. citizenship and reviews the DOD Personnel Security System of Record for any previous eligibility determination. If the employee's record shows a clearance as active, the company will need to assume ownership and determine if a background investigation is required to maintain eligibility. If the employee requires an upgrade to the level of a current eligibility, has never held a PCL, or previous access to classified information has been inactive for more than 24 months, this is referred to as an initial clearance. The FSO or security designee will initiate the process by submitting a clearance request via the DOD Personnel Security System of Record. The employee must furnish electronically a completed Security Questionnaire, signature on a certification, and all appropriate release forms and a current set of fingerprints for upload in an approved secure transmission system. Collectively, these documents are referred to as the security clearance package. The FSO reviews the security clearance package for adequacy and completeness before releasing it in the DOD Personnel Security System of Record to DCSA for vetting and interim PCL determination.

An investigator schedules the national security background investigation. If the package is incomplete, the FSO or the appropriate government branch will be notified. Once the investigation is completed, the results are submitted to the DCSA for adjudication and a final eligibility determination. For industry, if the clearance request is not clearly consistent with national security interests, the DCSA forwards the case to the DOHA to determine whether it is clearly consistent with the national interest to grant or continue national security eligibility for the employee. Let's look at each of these activities in more detail.

FSO Use of DOD System of Record

Prior to initiating the PCL process, the FSO verifies that the employee is a U.S. citizen by examining either the employee's birth certificate, passport, or any of the other acceptable proof of U.S. citizenship documents listed in the NISPOM. 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 Personnel Security System of Record to verify U.S. citizenship.

U.S. Citizenship verified by:

- Birth certificate
- Passport
- Other documents per NISPOM

× I-9 verification is NOT sufficient

× DOD Personnel Security System of Record is NOT sufficient

U.S. citizenship must be verified only if it is the employee's initial clearance. The FSO then

reviews the DOD Personnel Security System of Record for several aspects. First, the FSO determines whether or not the employee has a record present in the DOD Personnel Security System of Record. Then, if the employee does have a record in the DOD Personnel Security System of Record, the FSO determines whether or not the record shows a previous favorable eligibility determination to access classified information.

If the employee does have a previous favorable eligibility determination, the FSO assesses whether or not that determination may be accepted. If the determination may be accepted, the FSO must also assess if a background investigation is required to maintain eligibility. If an employee has no record in the DOD Personnel Security System of Record, and therefore no previous eligibility determination, then the FSO will establish a record for the employee in the DOD Personnel Security System of Record and initiate a PCL request. If the employee does have a record in the DOD Personnel Security System of Record but does not have a previous eligibility determination, then the FSO will initiate a PCL request for the employee in the DOD Personnel Security System of Record.

Review:

- If the employee has a record in the DOD Personnel Security System of record
- If the employee has previous favorable eligibility
- Assess if favorable eligibility can be accepted
- Determine if background investigation is required to maintain eligibility

Let's take a look at what factors the FSO evaluates in the PCL process.

Evaluating a Pre-Existing Eligibility Determination

A previous favorable eligibility determination may be accepted if it was issued by the federal agency currently requiring the employee 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 the NISPOM establish the requirements for reciprocity.

If a previous favorable eligibility determination meets or exceeds the requirement for reciprocity, then a PCL request is not needed. If a previous eligibility determination does not meet or exceed the requirement, then the FSO will need to initiate a PCL request.

PCL Request NOT Needed

The employee's FSO will NOT need to initiate a new PCL request if the previous National Security Background Investigation or eligibility determination if:

- Investigation/eligibility determination was issued by federal agency
- Determination was based on an investigation of a scope that meets or exceeds standards per the NISPOM for the level of access required

- Employee's last access to classified information has not exceeded 24 months
- Access to classified information may be granted to an employee without further investigation based on DCSA guidance

PCL Request Needed

The employee's FSO will need to initiate a new PCL request if the previous National Security Background Investigation or eligibility determination fails to meet any one of the required conditions.

- Investigation/eligibility determination was issued by a federal agency
- × Determination was based on an investigation of a scope that meets or exceeds standards per the NISPOM for the level of classified access required
  - Employee's last access to classified information has not exceeded 24 months
  - Access to classified information may be granted to an employee without further investigation based on DCSA guidance

Candidate Use of DOD Personnel Security System of Record

Remember Brenda, the new contractor employee who needs a PCL? To initiate the clearance process, Brenda's FSO, Mr. Fuller, checks the DOD Personnel Security System of Record and determines she does not have a record in that system. Therefore, he establishes a record for Brenda in the DOD Personnel Security System of Record and initiates a PCL request for her. Brenda can now electronically complete the Security Questionnaire.

Once she has fully completed the Security Questionnaire, Brenda must electronically submit the form with its certification and appropriate release forms so Mr. Fuller, her FSO, can access and review her documentation via the DOD Personnel Security System of Record. The forms that must be signed within the Security Questionnaire are the Security Questionnaire Certification, the Authorization for Release of Information, the Fair Credit Reporting Disclosure and Authorization, and, if appropriate, the Authorization for Release of Medical Information. If Brenda has not already done so, she will need to provide Mr. Fuller with a set of her fingerprints. Fingerprints are generally captured digitally and are uploaded by the FSO via an approved secure transmission system. The background investigation may not begin until the fingerprints are received by DCSA or the ISP. If the electronic fingerprints are not received within the required timeframe, the background investigation request will be rejected as incomplete, and the FSO is notified via the DOD Personnel Security System of Record.

FSO Review of Security Clearance Package

Now that Brenda has completed and submitted the Security Questionnaire, the signed certification, and appropriate release forms to Mr. Fuller, he can perform an FSO review of Brenda's security clearance package. As specified in the NISPOM, the FSO shall inform the

employee that the Security Questionnaire is subject to review to determine its adequacy and completeness. The NISPOM explicitly states the sole purpose of an FSO's review of the Security Questionnaire is to ensure adequacy and completeness only and that the information contained in a candidate's security clearance package cannot be used for any other purpose within the company. The Security Questionnaire is available for review on the Course Resources page.

Written notification on the Belacort Letterhead reads as follows, "The scope of this review is limited to determining the adequacy and completeness of your Security Questionnaire. The information contained in your Security Questionnaire 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 release the package in the DOD Personnel Security System of Record to DCSA for vetting and interim eligibility determination.

Retention of the Security Clearance Package

Electronic copies of the documents included in the security clearance package are submitted to DCSA via the DOD Personnel Security System of Record. Any hardcopies of the Security Questionnaire, certification, release forms, and other documents included in the security clearance package must be destroyed or returned to the employee to maintain. Because the Security Questionnaire is reviewed as part of Special Access Program (SAP) access determinations, the most current Security Questionnaire for employees 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.

Overview of Interim Reviews

Once the NISP PCL process has been initiated, and the employee's security clearance package has been released and fingerprints uploaded, the next stage of the PCL process may begin. In this stage of the PCL process, an interim review of the security clearance package is conducted by DCSA vetting to determine whether the employee will be granted an interim eligibility determination to access classified information. Once an interim eligibility determination has been made, DCSA will update the DOD Personnel Security System of Record accordingly and release the security clearance package to an investigator with DCSA or an ISP, who will then schedule the employee's national security background investigation.

Interim Review Process

All employees submitted for a PCL are routinely considered for interim eligibility determination. Interim eligibility permits the employee to access classified information, as appropriate, needed to perform his or her duties, pending the completion of the full national

security background investigation. The interim eligibility determination is granted and valid provided there is no evidence of adverse information that calls into question an employee's eligibility for classified access. Not all applicants are granted interim eligibility.

Overview of Personnel Security Investigations

Once a determination has been made regarding whether to grant the employee interim eligibility, the PCL process may begin. In this stage of the PCL process, the investigator from DCSA or an ISP conducts the appropriate national security background investigation. The investigator begins by confirming that the security clearance package received is complete. Next, the investigation is scheduled, then the investigator verifies 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

DCSA has received Brenda's security clearance package to review and vet. Before beginning Brenda's investigation, DCSA must first confirm that her security clearance package is complete and then make an interim eligibility determination. In this case, Brenda's security clearance package contains all the required information, and she has been vetted for an interim PCL, so Brenda's national security background investigation may begin. If, however, all the required information of the security clearance package had not been received within DCSA's required timeframe for receipt of the package, then the package would have been returned as incomplete, and the FSO would have been notified via the DOD Personnel Security System of Record. Upon receipt of the returned security clearance package, the employee is contacted by the FSO and provided with further instructions. If DCSA does not grant an interim PCL, DCSA will notify the FSO via the DOD Personnel Security System of Record, and the FSO will contact the employee about the decision. DCSA will then conduct a national security background investigation on the employee and determine a final eligibility.

Initial Investigations

Since DCSA has received Brenda's security clearance package and fingerprints and determined all to be complete, the appropriate background investigation will be conducted on Brenda. In a basic national security background investigation, national and local agency records, including credit and fingerprint records are checked, when appropriate, and the information provided by the employee such as addresses, employers, and schools are verified. Neighbors, supervisors and co-workers, classmates, and references, may also be contacted, if required, and law enforcement agencies in the places where the employee lived, worked, and attended school will be contacted. Further, the 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 employee, if required.

Five-Tiered Investigative Model

On June 30, 2008, President George W. Bush signed E.O. 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, the revised Federal Investigative Standards (FIS) were approved. The revised FIS established a new investigative model, which aligns and standardizes national security background investigation requirements for HSPD-12, suitability and fitness, and national security into 5 tiers. The 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. Tiers 3 and 5 are the national security background investigations used for PCLs to grant eligibility to classified information and/or assignment to a national security sensitive position.

Tier 3

Tier 3 national security background investigations are conducted for positions designated as non-critical sensitive, and/or requiring CONFIDENTIAL, SECRET, or "L" access eligibility. This tier of investigation requires completion of a Questionnaire for National Security Positions.

Tier 5

Tier 5 national security background investigations are conducted for positions designated as critical-sensitive or special-sensitive and/or requiring "Q" or TOP SECRET access or access to Sensitive Compartmented Information (SCI). This tier of investigation requires completion of a Questionnaire for National Security Positions.

Continuous Vetting

Once an employee receives a favorable eligibility to access classified information, the employee's background will be regularly reviewed to ensure they continue to meet security clearance requirements. This process is referred to as Continuous Vetting, or CV. The CV process is a risk-managed approach with select automated records checks that reviews an employee's background at any time during an individual's period of eligibility. It helps employees and DCSA to address and mitigate personnel security situations before they become larger problems. To maintain eligibility, the employee will need to complete a Security Questionnaire every five years, regardless of eligibility level. The investigation request will be screened using a risk-management based approach, where the Security Questionnaire is analyzed and identified for either enrollment in CV or submission for an investigation. Once this is determined, DCSA will update the DOD Personnel Security System of Record accordingly.

Overview of Adjudicative Process

After the employee's national security background investigation is completed, the results of the background investigation are forwarded to the DCSA for adjudication. The DCSA will determine a final eligibility in accordance with the Office of the Director of National Intelligence (ODNI) Security Executive Agent Directive (SEAD) 4, National Security Adjudicative Guidelines. The decision is based on review and consideration from results and other available, reliable information collected from the national security background investigation. Once the eligibility determination has been made, the employee 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 to grant eligibility. The whole person concept involves carefully assessing all the available information about an individual, both favorable and unfavorable, from the individual's past and present. The individual'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 using a standardized set of national security adjudicative guidelines to ensure all individuals 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 when an individual is reviewed under a guideline, both disqualifying and mitigating information is considered. Each guideline addresses a specific concern that can impact an individual's ability to protect national security.

Review each guideline to learn about the concern associated with it. For more detailed information about the adjudicative process, refer to the SEAD 4, National Security Adjudicative Guidelines, Job Aid on the Course Resources page.

Term	Definition/Explanation	Concern
Guideline A	Allegiance to the U.S.	The willingness to safeguard classified or sensitive information is in doubt if there is any reason to suspect an individual's allegiance to the U.S. Negative indicators include an individual who participates in or supports for acts against the U.S. or places the welfare or interests of another country above those of the U.S. An individual who engages in acts against the U.S. or provides support or encouragement to those who do has already demonstrated willingness to compromise national security.
Guideline B	Foreign Influence	Foreign contacts and interests are a national security concern if they result in divided allegiance. They may create circumstances in which the individual may be manipulated or induced to help a foreign person, group, organization, or government in a way inconsistent with U.S. interests or otherwise made vulnerable to pressure or coercion by any foreign interest.
Guideline C	Foreign Preference	When individuals act in such a way as to indicate a preference for a foreign country over the U.S., then they may provide information or make decisions that are harmful to the interests of the United States. Foreign involvement raises concerns about an individual's judgment, reliability, and trustworthiness when it is in conflict with U.S. national interests or when the individual acts to conceal it.
Guideline D	Sexual Behavior	Sexual behavior that involves a criminal offense reflects a lack of judgment or discretion or may subject the individual to undue influence of coercion, exploitation, or duress. These issues can raise questions about an individual's judgment, reliability, trustworthiness, and ability to protect classified or sensitive information.

Term	Definition/Explanation	Concern
Guideline E	Personal Conduct	Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information.
Guideline F	Financial Considerations	Failure to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control and lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. An individual who is financially overextended is at greater risk of having to engage in illegal or otherwise questionable acts to generate funds.
Guideline G	Alcohol Consumption	Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses and can raise questions about an individual's reliability and trustworthiness.
Guideline H	Drug Involvement and Substance Misuse	The illegal use of controlled substances, to include the misuse of prescription and non-prescription drugs, and the use of other substances that cause physical or mental impairment or are used in a manner inconsistent with their intended purpose can raise questions about an individual's reliability and trustworthiness, both because such behavior may lead to physical or psychological impairment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.
Guideline I	Psychological Conditions	Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness.

Term	Definition/Explanation	Concern
Guideline J	Criminal Conduct	Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules, and regulations.
Guideline K	Handling Protected Information	Deliberate or negligent failure to comply with rules and regulations for handling protected information that includes classified and other sensitive government information and proprietary information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information and is a serious security concern.
Guideline L	Outside Activities	Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified or sensitive information.
Guideline M	Use of Information Technology	Failure to comply with rules, procedures, guidelines, or regulations pertaining to IT systems may raise serious concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information.

Roles of DCSA Adjudications

What about Brenda and her application for eligibility? Let's see how it's going. The DCSA investigator or an ISP has completed its national security background investigation on Brenda and has forwarded the results for adjudication and a final eligibility determination. The adjudicator at DCSA reviewed and considered the investigation results. By applying the national security 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 DCSA makes an unfavorable adjudicative determination, then the contractor employee 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 employee notified? Regardless of whether the eligibility determination was granted or denied, the decision is recorded in the DOD Personnel Security System of Record and the employee's FSO is notified via the DOD Personnel Security System of Record. The FSO, in turn, notifies the employee.

Review Activity 1

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

Question 1 of 4

Step 1

- Completes Security Questionnaire
- Handles a contractor employee's appeal of an unfavorable adjudicative determination
- Vets and adjudicates background investigation results for final eligibility
- Initiates the PCL request

Answer: Initiates the PCL request

Question 2 of 4

Step 2

- Completes Security Questionnaire
- Handles a contractor employee's appeal of an unfavorable adjudicative determination
- Vets and adjudicates background investigation results for final eligibility
- Initiates the PCL request

- **Answer:** Completes Security Questionnaire

Question 3 of 4

Step 3

- Completes Security Questionnaire
- Handles a contractor employee's appeal of an unfavorable adjudicative determination
- Vets and adjudicates background investigation results for final eligibility
- Initiates the PCL request

Answer: Vets and adjudicates background investigation results for final eligibility

Question 4 of 4

Step 4

- Completes Security Questionnaire
- Handles a contractor employee's appeal of an unfavorable adjudicative determination
- Vets and adjudicates background investigation results for final eligibility
- Initiates the PCL request

Answer: Handles a contractor employee's appeal of an unfavorable adjudicative determination

Review Activity 2

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

Question 1 of 5
Initiates the PCL request

- FSO
- DCSA
- Investigator
- Employee
- DOHA

Answer: The FSO uses the DOD Personnel Security System of Record to initiate the PCL Request.

Question 2 of 5
Completes Security Questionnaire

- FSO
- DCSA
- Investigator
- Employee
- DOHA

Answer: Employees must provide information about themselves by electronically completing a Security Questionnaire.

Question 3 of 5
Vets the security clearance package and adjudicates background investigation results for final eligibility

- FSO
- DCSA
- Investigator
- Employee
- DOHA

Answer: DCSA vets the submitted security clearance package for an interim PCL. After the employee's national security background investigation is completed, the results are forwarded to DCSA for adjudication and final eligibility determination.

Question 4 of 5
Conducts a national security background investigation on the individual

- FSO
- DCSA
- Investigator
- Employee
- DOHA

Answer: The investigator with DCSA or an ISP conducts the appropriate background investigation.

Question 5 of 5
Handles a contractor employee's appeal of an unfavorable adjudication determination.

- FSO
- DCSA
- Investigator
- Employee
- DOHA

Answer: If the DCSA makes an unfavorable adjudicative determination, then the contractor employee may appeal the determination to DOHA.

Review Activity 3

What do you know about how information is obtained and submitted during the PCL process?

Question 1 of 4
Which of the following is reviewed by the FSO to determine if a candidate has a previous favorable eligibility determination?

- DOD Personnel Security System of Record
- Security Questionnaire

Answer: The FSO reviews the DOD Personnel Security System of Record to determine if the employee has a previous favorable eligibility determination.

Question 2 of 4
Which of the following is used to record the eligibility determination?

- DOD Personnel Security System of Record
- Security Questionnaire

Answer: The DOD Personnel Security System of Record is used to record the eligibility determination.

Question 3 of 4
Who of the following completes the Security Questionnaire?

- FSO
- Employee

Answer: The employee completes the Security Questionnaire.

Question 4 of 4
Who of the following verifies the employee's U.S. citizenship?

- Employee
- FSO

Answer: The FSO verifies the employee's U.S. citizenship.

Review Activity 4

Of the following, which of the items below correctly list each definition?

Question 1 of 4
Positions requiring the completion of Questionnaire for National Security Positions

- Tier 3
- Tier 5
- Tier 3 and Tier 5
- Continuous Vetting (CV)

Answer: Tier 3 and Tier 5 investigations require completion of a Questionnaire for National Security Positions.

Question 2 of 4
Positions requiring CONFIDENTIAL, SECRET, or "L" (Department of Energy or DOE) Access Eligibility

- Tier 3
- Tier 5
- Tier 3 and Tier 5
- Continuous Vetting (CV)

Answer: Tier 3 national security background investigations are conducted for positions designated as non-critical sensitive, and/or requiring CONFIDENTIAL, SECRET, or "L" access eligibility.

Question 3 of 4
Positions requiring TOP SECRET, Sensitive Compartmented Information (SCI), or "Q" (Department of Energy or DOE) Access Eligibility

- Tier 3
- Tier 5
- Tier 3 and Tier 5
- Continuous Vetting (CV)

Answer: Tier 5 national security background investigations are conducted for positions designated as critical-sensitive to special-sensitive and/or requiring "Q" or TOP SECRET access or access to Sensitive Compartmented Information, or SCI.

Question 4 of 4
Risk-managed approach that reviews an employee's background at any time during an individual's period of eligibility.

- Tier 3
- Tier 5
- Tier 3 and Tier 5
- Continuous Vetting (CV)

Answer: Continuous Vetting (CV) is a risk-managed approach with select automated records checks that reviews an employee's background at any time during an individual's period of eligibility.

Review Activity 5
What do you know about how a subject's application is adjudicated?

Question 1 of 2

Which of the following assesses both favorable and unfavorable information from both an individual's past and present?

- Whole Person Concept
- National Security Adjudicative Guidelines

Answer: 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.

Question 2 of 2
Which of the following ensures all individuals are assessed using the same standardized criteria?

- Whole Person Concept
- National Security Adjudicative Guidelines

Answer: To conduct a review that is fair and free of bias, adjudicators utilize national security adjudicative guidelines when evaluating the results of an individual's national security background investigation.

Lesson 4: Managing the PSP at a Cleared Facility

Lesson Objective

Managing the PSP at a cleared facility involves more than obtaining PCLs. Cleared employees must receive required security briefings at specified intervals and employee eligibility and access records must be reviewed on a continuous basis.

In this lesson, you will learn the PSP key managing elements at a cleared facility.
Here is the lesson objective:

- Identify Personnel Security Program key managing elements at a cleared facility.

Security Briefings Overview

Brenda's PCL request has been processed and her eligibility has been adjudicated and favorably determined. While it may appear the PCL process ends when the employee receives a favorable eligibility determination, there are more requirements to complete. As you learned earlier, although Brenda has eligibility, one of the other requirements she must meet in order to obtain access to classified information is to receive the appropriate security briefing and, when applicable, security education and training.

Security Training

Security education and training ensures cleared individuals are aware of their roles 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 eligibility determination for the first time, and is required to be completed prior to granting the individual classified access. This training includes a threat awareness briefing, including insider threat; a counterintelligence (CI) awareness briefing; an overview of the security classification system; a discussion of employee reporting obligations and requirements, including insider threat; cybersecurity awareness training; and a discussion of the security procedures and duties applicable to an employee's job.

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 about changes in security regulations and policies.

Limiting Access

Recall that in order to access classified materials, a cleared individual must work at a cleared

facility. FCLs and PCLs impact each other. As with PCLs, in order to obtain an FCL, the company must require access to classified information, and this requirement must be verified. If the highest level of classified access required by Belacort's classified contract is SECRET, then Belacort's FCL will be issued at the SECRET level and no higher. This means any employee who is granted an initial eligibility determination while working for Belacort will only be cleared 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 classified access is limited by their employing company's FCL level. This means even if an employee has a previous TOP SECRET PCL eligibility, if the facility's FCL is only at the SECRET level, then the employee may only access information classified at the SECRET level or below while performing classified work for that company.

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 the required KMP either receiving PCLs or completing exclusion resolutions. KMP, such as the SMO, the ITPSO, and the FSO must be cleared to the same level as the FCL before a final FCL will be granted. Other KMPs and employees supporting a classified contract 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. KMPs not required to be cleared in connection with the FCL may be formally excluded from classified access by executing the associated exclusion resolution. For more information on the FCL process, please refer to the Facility Clearances in the NISP course on the Course Resources page.

Overview

Recall that in order to access classified information, an individual must have favorable eligibility for access to classified information at the appropriate level, have a valid need-to-know for the classified information being accessed, a signed nondisclosure agreement, or SF 312, and receive an initial security briefing per the NISPOM.

Once access has been granted, the FSO is responsible for reviewing and maintaining the accuracy of their employee's security access records on a continuing basis. This review should also ensure their cleared employees still have a valid requirement to access classified information. FSOs must determine when an employee is required to complete an updated Security Questionnaire and report required information as applicable.

Upon notification of denial, revocation, or suspension of an employee's PCL, FSOs are required to immediately deny that employee access to classified information.

Eligibility determinations do not expire. While an employee may have received a favorable initial eligibility determination, to be allowed continued access to classified information, the employee must complete the Security Questionnaire, regardless of eligibility level, and undergo a background investigation for the maintenance of their eligibility every five years. As mentioned earlier, this process is referred to as Continuous Vetting, or (CV), a risk-managed approach which helps employees and DCSA address and mitigate personnel security situations before they become larger problems. The FSO will run a report on their cleared employees in the DOD Personnel Security System of Record to determine who is due to complete an updated Security Questionnaire. The FSO then reviews records to ensure that the employee still requires access to classified information. If the employee does still requires classified access, the employee will receive an eligibility maintenance requirement notification, generally via email from the FSO and the government agency responsible for the background investigation system of record. The notifications will include instructions and guidance about the personnel background investigation required as part of the CV process and the system of record used to update their Security Questionnaire.. If the employee does not still require classified access, an updated Security Questionnaire is not required and the employee will be debriefed from classified access. The employee's record will be updated accordingly in the DOD Personnel Security System of Record.

Reporting Required Information

To maintain current information on cleared employees, FSOs must report required information appropriately. The NISPOM provides reporting requirements and obligations. In general, FSOs must report events or information that have an effect on the status of the FCL, have an effect on the status of an employee's PCL, events that indicate the employee poses an insider threat, affect proper safeguarding of classified information, or indicate classified information has been or is suspected to be lost or compromised. For more information on the contractor's requirements to report certain information, refer to the NISP Reporting Requirements course on the Course Resources page.

PCL Reporting Requirements

Information that may affect an individual's PCL is reported to DCSA. FSOs are required to report adverse information concerning a cleared employee, including insider threat behaviors, which is relevant and credible information indicative of a potential or actual insider threat that is covered by any of the national security adjudicative guidelines; any suspicious contacts; an employee desiring not to be processed for a PCL, or not to perform on classified work; an employee refusing to sign the Classified Information Nondisclosure Agreement (SF 312); and any change in the status of a cleared employee, such as death, name change, change in citizenship, including when a non-U.S. citizen granted Limited Access Authorization (LAA) becomes a citizen through naturalization, unofficial foreign travel, termination of

employment, Individual Culpability Reports on employees who violate security requirements, change conditions affecting the FCL, and the loss, compromise, or suspected compromise of classified material must also be reported to DCSA.

Review Activity 1

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

Question 1 of 3

Once applicants receive a favorable national security eligibility determination, they may access classified information immediately.

- True
- False

Answer: False. Although an individual may be granted eligibility, they also must have a need-to-know for the classified information being accessed, a signed nondisclosure agreement, or SF 312, and receive an initial security briefing.

Question 2 of 3

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

- True
- False

Answer: False. Eligibility determinations do not expire; however, to maintain eligibility, the employee will need to complete a Security Questionnaire every five years, regardless of level.

Question 3 of 3

The employee does not have to undergo a background investigation for the maintenance of their eligibility.

- True
- False

Answer: False. The employee will need to undergo a background investigation for the maintenance of their eligibility. This process is referred to as Continuous Vetting, or (CV).

Review Activity 2

Let's check your knowledge.

Question 1 of 3

Cleared employees must receive security refresher training _____.

- annually
- bi-annually
- not required

Answer: Once cleared individuals have received initial security briefing and held a clearance for one year, they must receive security refresher training at least annually.

Question 2 of 3

FSOs are responsible for providing _____ to the cleared personnel employed at their facility.

- both initial security briefings and refresher security training
- initial security briefings only
- refresher training only

Answer: Facility Security Officers (FSOs) are responsible for providing BOTH initial security briefings and refresher security training to the cleared personnel employed at their facility.

Question 3 of 3

KMP that must be cleared to the same level as the FCL are the:

- FSO, Program Manager, SMO
- SMO, FSO, ITPSO
- ITPSO, SMO, Program Manager

Answer: Key Management Personnel (KMP) that must be cleared to the same level as the FCL are the Senior Management Official (SMO), Facility Security Officer (FSO), and the Insider Threat Program Senior Official (ITPSO).

Lesson 5: Personnel Clearances Challenge

Getting Started

Welcome to the Personnel Clearances Challenge. This challenge will give you a chance to practice identifying what is required in the PSP at cleared facilities. Here's how it works. As the FSO, you'll make decisions regarding the management of the PSP. You will review items in your office, such as file folders and email messages. When you review each one, you'll see a question related to the PSP.

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

You check the DOD Personnel Security System of Record to determine the eligibility status of each employee required to access classified material on this new SECRET contract. You see that Brian, the instructional designer, has an active SECRET PCL; Diane, the new digital artist, has no record in the DOD Personnel Security System of Record and has never had a national security eligibility determination.

Determine which answer is correct.

- ○ Only Diane requires a SECRET PCL at this time and must be initiated for one.
- ○ Neither Brian nor Diane requires a SECRET PCL at this time.
- ○ Brian may perform classified work on the contract now since he has an active SECRET PCL, but Diane requires a SECRET PCL and must be initiated for one.

Answer: Brian may perform classified work on the contract now since he has an active SECRET PCL, but Diane requires a SECRET PCL and must be initiated for one.

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 Security Questionnaire for National Security Positions?

Select all that apply.

- ☐ Verify that Lindsay is a U.S. citizen
- ☐ Review DOD Personnel Security System of Record for previous eligibility determination
- ☐ Assess if a background investigation is required to maintain eligibility
- ☐ Initiate PCL request via the DOD Personnel Security System of Record

Answer: You will need to verify Lindsay is a U.S. citizen and review the DOD Personnel Security System of Record to see if Lindsay has a previous eligibility determination. Then, you will need to assess whether a background investigation is required to maintain eligibility. Next, you will need to initiate Lindsay's PCL request using the DOD Personnel Security System of Record.

Folder: Information about Employee

Someone has left a blank manila folder on your desk. You review the folder. It looks like Lindsay does not want to sign the Classified Information Nondisclosure Agreement, or 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.

- ○ You should submit a report via the DOD Personnel Security System of Record about Lindsay 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

Answer: You should submit a report via the DOD Personnel Security System of Record. FSOs are required to report a cleared employee refusing to sign the Classified Information Nondisclosure Agreement, or SF 312, and employees desiring not to perform on classified work.

Question 2

To whom should you submit the report about Lindsay refusing to sign the SF 312?

Determine which answer is correct.

- ○ DOE
- ○ DCSA
- ○ DOHA

Answer: You will need to submit the report to DCSA.

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 and Senior Management Official (SMO) of your company. Julie has never had a PCL. Will you need to initiate the PCL 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 (FCL)
- ○ No, Julie's position is not one that requires her to be cleared in connection with the FCL
- ○ No, Julie does not need a PCL since she will not be working directly on the classified contract

Answer: Yes, Julie will need a PCL equivalent to that of your company's FCL as she now holds a KMP position that is required to be cleared in connection with the FCL.

Folder: Security Education and Training

Now you review the folder labeled Security Education and Training. There are two documents inside the folder labeled Initial Security Briefing and Refresher Security Training. Once all the employees who will be working on the classified contract have received their initial PCL, you must ensure they are aware of their roles and responsibilities regarding the safeguarding of classified materials.

Question 1: Initial Security Briefing

What must you include in the initial security briefing for the employees with new personnel security clearances, or PCLs?

Select all that apply.

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

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

Lesson 6: Course Conclusion

Course Summary

PCLs, as part of 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 employee, conducting a national security background investigation of the employee, and reviewing and considering the results of that investigation to make a final eligibility determination.

The contractor's responsibility under the PSP does not end with the issuance of a favorable eligibility determination. Maintaining a PCL and managing the PSP program at a cleared contractor facility involves reviewing and maintaining the accuracy of their employee's security access records on a continuous basis and ensuring their cleared employees still have a valid requirement to access classified information.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- Overview of Personnel Clearances in the NISP
- Processing NISP 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 roles of various government components in the NISP Personnel Security Clearance process for contractors
- Identify entity and individual responsibilities in the eligibility processing of Personnel Security Clearances
- Identify the basic and common functions of the DOD Personnel Security System of Record
- Identify the investigative model used to make national security eligibility

determinations and the Continuous Vetting process

- Identify the national security adjudicative guidelines for the Personnel Security Program
- Identify Personnel Security Program key managing elements at a cleared facility

To receive course credit, you MUST take the Personnel Clearances in the NISP examination. Please register for the online exam in the Security, Training, Education, and Professionalization Portal (STEPP) system from the Center for Development of Security Excellence (CDSE) website.