Introduction to Personnel Security Student Guide

27 May 2020

Center for Development of Security Excellence

Introduction to Personnel Security

Lesson 1: Course Introduction

The objective of the Personnel Security Program is to make a reasonable determination that individuals granted access to classified information or assigned to sensitive positions are and will remain loyal, trustworthy, and reliable.

Consequently, all security specialists are tasked with understanding the Personnel Security Program, or PSP. It is necessary to have a thorough understanding of its origins and processes.

Course Objectives:

- Demonstrate comprehension of the Personnel Security Program (PSP).
- Explain National Security sensitive position designations and special access requirements.
- Apply investigative process and comprehend the national security adjudication requirements.
- Identify security specialist's responsibilities under the PSP.
- Analyze the continuous evaluation and reinvestigation requirements.

Course Lessons:

- Course Introduction
- The Personnel Security Program
- Position Designations and Special Access Requirements
- Investigation and Adjudication
- Investigative Service Providers and Record Keeping
- Continuous Evaluation and Reinvestigation
- The Security Specialist
- Course Summary

Lesson 2: The Personnel Security Program

This lesson will cover the definition and purpose of personnel security, PSP history, personnel security policies, and major components of the PSP.

Lesson Objectives:

- Comprehend the definition and purpose of personnel security
- Explain the history behind the creation of the Personnel Security Program (PSP)
- Identify personnel security policy
- Identify the major components of the PSP

The Purpose of the Personnel Security Program

The PSP aims to protect national security by ensuring that only loyal, trustworthy, and reliable individuals may access classified information and/or be assigned to national security sensitive positions.

The PSP establishes the standards, criteria, and guidelines upon which personnel security determinations are based. The PSP uses a comprehensive background investigative process to make this determination.

The investigative process applies to members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated people who require access to classified information or who are assigned national security sensitive duties.

The goal of the PSP is to ensure the protection of national security. Two key aspects of the PSP – providing access to classified information and ensuring the protection of national security.

Access to Classified Information

Unauthorized disclosure of classified or sensitive information can cause significant harm to national security. Information that requires special protection is known as national security information and may be designated as "classified."

In the U.S., there are three levels of classified information: Top Secret, Secret, and Confidential. The degree of damage to national security that could result from its unauthorized disclosure determines which classification applies.

Top Secret is the highest level of classification. It applies to information that reasonably could be expected to cause exceptionally grave damage to the national security if unauthorized disclosure occurs.

Secret classification applies to information that could be expected to cause serious damage to the national security if unauthorized disclosure occurs. Confidential classification applies to information that reasonably could be expected to cause damage to the national security if

unauthorized disclosure occurs.

National security encompasses both the national defense and the foreign relations of the U.S. which must be protected from harmful individuals, organizations, and nations.

One way a nation can defend itself is to maintain a good working relationship with other countries, thereby reducing threats to our nation's survival. Unfortunately, some national security threats faced by the United States come from individuals who are already inside.

These are known as insider threats. Therefore, assigning individuals who possess a history of being loyal, trustworthy, and reliable to sensitive positions is critical to protecting and maintaining our national security.

Character Traits of Cleared Employees

The United States Government expects cleared employees to be loyal, trustworthy, and reliable. But, how do we determine if individuals with a need to access national security information possess these traits?

Three questions are asked of everyone who has a need for access to classified or sensitive information. Is the individual's allegiance solely with the United States and its basic form of Government? Can the individual be trusted to properly protect classified information and/or perform other sensitive duties? Is the individual consistently willing and able to carry out security responsibilities?

The answer to all of the above questions should be yes.

The History of the PSP

This Course will also cover the history of the PSP to better understand what it has become today. Prior to the Civil Service Act of 1883, federal employees, even at the lowest levels, were political appointees.

The system by which people were appointed to civil service jobs was called the **Spoils System**. This system required allegiance to the party boss and the political party that appointed you, as opposed to a larger sense of allegiance to the Constitution. The employee was presumed to be loyal because in the past, he or she was loyal to the party and the party boss. The employee won the job as a favor from the party and could only keep it by staying in the party's favor. This provided a powerful impetus to keep employees 'party-loyal'.

Because of the many abuses of the Spoils System, such as incompetent and corrupt political officials, or civil servants who felt they were working for the party rather than the American people, Congress passed the Civil Service Act in 1883.

The **Civil Service Act** created the U.S. Civil Service Commission. The act required employees be appointed on the basis of ability, which was demonstrated by taking an exam. This created

uncertainty about the partisan allegiance of federal employees who were no longer dependent upon the party favor to keep their jobs. Their party loyalty could no longer be 'bought' or necessarily even depended upon.

Eventually, Congress passed the **Hatch Act of 1939**, which limits certain political activities of Federal employees. It ensures administration of federal programs in a nonpartisan fashion. Moreover, the Hatch Act protects Federal employees from political coercion in the workplace. It makes certain that Federal employees receive advancement based on merit and not based on political affiliation.

Executive Orders, Policies, Regulations, and Guidelines

The Personnel Security Program is governed by several executive orders, or E.O.s, policies, regulations, and guidelines.

Executive Orders: E.O. 10450

E.O. 10450, Security Requirements for Government Employment, establishes security requirements for government employment. Each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined according to the degree of adverse effect on the national security that the occupant of the position could bring about,

Executive Orders: E.O. 10865
E.O. 10865, Safeguarding Classified Information within Industry, requires all persons who are employed by the departments and agencies of the government to be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.

Executive Orders: E.O. 12968

E.O. 12968, Access to Classified Information and Background Investigative Standards, establishes a uniform federal Personnel Security Program for employees who are considered for initial or continued access to classified information. This order also establishes Security policies designed to protect classified information.

Executive Orders: E.O. 13467

E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. This executive order authorizes the continued evaluation of personnel who hold an active national security eligibility determination. It designates the Director of National Intelligence as the "**Security Executive Agent**" (SecEA) with responsibility over security and public trust clearance processing, and the Office of Personnel Management as the "Suitability Executive Agent" with continued responsibility and authority for federal employment suitability investigations and determinations and authorizes continuous evaluation of personnel who hold an active national security clearance.

Executive Orders: E.O. 13764

E.O. 13764, Amended the Civil Service Rules, was directed toward amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability, and Fitness for Employment and Credentialing, and related matters.

Security Executive Agent Directives (SEADs)

There are three Security Executive Agency Directives, or SEADs, that are important in governing the PSP.

SEAD 3 - Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. This Directive does not limit the authority of agency heads to impose additional reporting requirements in accordance with their respective authorities under law or regulation.

SEAD 4 - National Security Adjudicative Guidelines, establishes the single, common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. National Security Guidelines contained in SEAD 4 supersede all previously issued national security adjudicative criteria or guidelines. Appendix B of SEAD 4 contains the language of the Bond Amendment.

SEAD 6 - Continuous Evaluation, reforms processes related to suitability for government employment, fitness for contractor employees, and eligibility for access to classified national security information. Specifically, SEAD 6 establishes policy and requirements for the continuous evaluation (CE) of individuals who require continued eligibility for access to classified information or eligibility to hold a sensitive position.

CE modernizes the background investigation process by maximizing automated records checks to identify adjudicative relevant information to assist in assessing the continued eligibility of individuals at any time during their period of eligibility.

Bond Amendment

Passed in 2008, the Bond Amendment repealed Title 10 U.S.C. Section 996 (formerly known as the Smith Amendment) and placed restrictions that are similar to the Smith Amendment, but which apply to all Federal Government Agencies. The Bond Amendment bars persons from holding a national security eligibility for access to Special Access programs (SAPs), Restricted Data, and Sensitive Compartmented Information (SCI), if they have been convicted of a crime and served more than one year of incarceration, were discharged from the Armed Forces under dishonorable conditions, or were determined to be mentally incompetent by a court or administrative agency.

DoD Regulations

DoD Instruction 5200.02, The Personnel Security Program, establishes policies, assigns responsibilities, and prescribes procedures for the DoD Personnel Security Program, or PSP.

DoD Manual 5200.02, Procedures for the DoD Personnel Security Program, assigns responsibilities and prescribes procedures for investigations of individuals seeking to hold national security positions or perform national security duties and who are required to complete Standard Form 86, also called the SF 86 "Questionnaire for National Security Positions," for personnel security investigations or PSIs. The manual also sets procedures for DoD PSP national security eligibility for access determinations; personnel security actions; continuous evaluation, or CE, and security education requirements for employees seeking eligibility for access to classified information or to hold a sensitive position, referred to in this manual as "national security eligibility".

Federal Investigative Standards

The **Federal Investigative Standards**, also known as **FIS,** directed development of a five-tiered investigative model. This model established standard requirements for conducting national security background investigations to determine eligibility for access to classified information, to hold a national security sensitive position, for Federal Government employment, and access to Federal Government-controlled facilities.

PSP Components

The major components to the PSP are Designation, Investigation, Adjudication, Continuous Evaluation, and Reinvestigation.

Designation

Each position in the Federal service must be evaluated for a position sensitivity designation commensurate with the responsibilities and assignments of the position as it relates to the impact on the national security. Such responsibilities and assignments include, but are not limited to, access to classified information that is Confidential, Secret, or Top Secret, and any other duties by which the occupant could bring about a material adverse effect on the national security by virtue of the nature of the position.

Positions designated as “sensitive” involve job duties that can have a great impact on national security. Positions with job duties which have no potential for material adverse effect on national security are designated as nonsensitive.

Investigation

Once an individual is selected for a sensitive position and/or requires access to classified information a national security background investigation is conducted on the individual. The requisite FIS investigation depends on the position designation and risk or sensitivity level.

The national security background investigation obtains background information about the person that will hold a sensitive position. Once completed the information is transmitted to an adjudicative facility for adjudication.

Adjudication

Adjudication is an evaluation of the information contained in the national security background investigations and other source documents. Analysis and evaluation of reported information against the 13 National Security Adjudicative Guidelines determine an individual's national security eligibility.

National security adjudicators assigned to the DoD Consolidated Adjudications Facility, better known as CAF, provide the majority of national security eligibility determinations.

Continuous Evaluation

Once a covered individual receives eligibility for access to classified information or holds a national security sensitive position during the period of eligibility, an ongoing process of Continuous Evaluation, or CE.

CE is an ongoing personnel security investigative process utilized to review and monitor the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility..

CE leverages a set of automated records checks and business rules to assist in the ongoing assessment of an individual's continued eligibility.

Reinvestigation

National security eligibility or access becomes the basis of periodic reinvestigation, which is executed at predetermined intervals. Individuals are periodically reinvestigated at certain intervals based on their national security eligibility or access. However, reinvestigations may begin at any time unfavorable information emerges to raise concern under the National Security Adjudicative Guidelines. Reinvestigation is also a component of the Continuous Evaluation Program.

Knowledge Check

Question 1 of 3
Match the term to its description.
_____ Character traits looked for in a government employee
_____ System that required allegiance to a political party and not the Constitution
_____ Employees appointed based on ability
_____ Protects federal employees from political coercion in the workplace

A. Spoils System
B. Loyal, trustworthy, reliable
C. Civil Service Act
D. Hatch Act of 1939

Question 2 of 3

_____ Authorizes the continued evaluation of personnel who hold an active national security eligibility determination.
_____ Establishes adjudicative criteria for covered individuals who require eligibility for access to classified information or eligibility to hold a sensitive position.
_____ Maintains that DoD and Agency employees are reliable and trustworthy.
_____ Establishes the policy, assigns responsibilities, and prescribes procedures for the DoD Personnel Security Program.

A. E.O. 10865
B. DoDI 5200.02
C. E.O. 13467
D. SEAD 4

Question 3 of 3

_____ An assessment of a position's potential impact on the national security
_____ A national security eligibility determination made by evaluating the information in the national security background investigation against national standards
_____ A part of the CE Program that happens at certain intervals based on position designation or access
_____ A report used to make a national security eligibility determination
_____ A process that monitors employees for new information or changes that could affect an individual's national security eligibility

A. Continuous Evaluation
B. Reinvestigation
C. Adjudication
D. Investigation
E. Designation

Answers

Question 1 of 3
Match the term to its description.
_B___ Character traits looked for in a government employee
_A___ System that required allegiance to a political party and not the Constitution
_C___ Employees appointed based on ability
_D___ Protects federal employees from political coercion in the workplace

A. Spoils System
B. Loyal, trustworthy, reliable
C. Civil Service Act
D. Hatch Act of 1939
Answer: B, A, C, D

Question 2 of 3
_ C__ Authorizes the continued evaluation of personnel who hold an active national security eligibility determination.
_ D__ Establishes adjudicative criteria for covered individuals who require eligibility for access to classified information or eligibility to hold a sensitive position.
_ A__ Maintains that DoD and Agency employees are reliable and trustworthy.
_ B__ Establishes the policy, assigns responsibilities, and prescribes procedures for the DoD Personnel Security Program.

A. E.O. 10865
B. DoDI 5200.02
C. E.O. 13467
D. SEAD 4
Answer: C, D, A, B

Question 3 of 3
_E___ An assessment of a position's potential impact on the national security
_C___ A national security eligibility determination made by evaluating the information in the national security background investigation against national standards
_B___ A part of the CE Program that happens at certain intervals based on position designation or access
_D___ A report used to make a national security eligibility determination
_A___ A process that monitors employees for new information or changes that could affect an individual's national security eligibility

A. Continuous Evaluation
B. Reinvestigation
C. Adjudication
D. Investigation
E. Designation
Answer: E, C, B, D, A

The Personnel Security Program Summary

This lesson covered the purpose and history of the PSP, personnel security policy, and major components of the PSP. At this point, you should have an understanding of how the Personnel Security Program has evolved and why it is so important.

Remember, the PSP seeks to ensure only loyal, trustworthy, and reliable individuals receive eligibility to access classified information or assignment to national security sensitive duties.

The bottom line is to protect national security by employing those individuals who meet the standards, criteria, and guidelines of the Personnel Security Program.

Lesson 3: Position Designation and Special Access Requirements

This lesson will cover national security sensitive position designations, requirements for access to classified information including assignment to sensitive positions, and special access requirements.

Lesson Objectives:

- Comprehend national security sensitive position designations
- Identify the requirements to access classified information including assignment to a sensitive position
- Recognize the different special access requirements

Access

Designated positions correlate to the potentially adverse impact on national security. Access is the ability and opportunity to gain knowledge of classified information. This involves seeing, hearing, or touching classified information, material, or equipment.

The holder of information always controls access to the information or material. Therefore, the holder of the classified national security information has the responsibility to determine if the person seeking access has appropriate national security eligibility, access, and a valid need-to-know for the information in order to carry out their official duties.

To obtain a national security eligibility, you have to obtain a favorable determination. Component and local organization procedures provide guidance on how to verify national security eligibility and need-to-know.

Types of Access

Not just anyone can access classified information. There are two basic types of authorizations for granting access depending on whether you are a U.S. citizen or a non-U.S. citizen. If an individual is a U.S. citizen, that individual may receive national security eligibility.

If an individual is not a U.S. citizen, that individual may receive a Limited Access Authorization, also known as an LAA. These two authorizations may be granted to civilian, military, and contractor personnel; however, their requirements for access will vary.

It is important to understand that although a non-U.S. citizen may receive an LAA, a non-U.S. citizen is not granted national security eligibility.

Designation Categories

Civilian personnel designation requirements vary based on how the position is categorized. OPM defines the four civilian position sensitivity levels as special-sensitive, critical-sensitive, noncritical-sensitive, and nonsensitive.

When there is a mix of duties, the highest level of duty determines the sensitivity. The designation of sensitive positions meets the stated criteria for a specific security designation and is necessary to meet mission requirements.

Special-Sensitive

Special-sensitive national security positions are civilian national security positions that may potentially cause inestimable damage to the national security or adverse impact to the efficiency of the DoD or military services. This includes positions requiring eligibility for access to sensitive compartmented information or SCI, positions requiring eligibility for access to unique or uniquely produced intelligence-related special-sensitive information or involvement with special access programs, or SAPs, and any civilian position the DoD Component head determines to be a higher level than critical-sensitive due to its special requirements.

Critical-Sensitive

Critical-sensitive positions are civilian national security positions that have the potential to cause exceptionally grave damage to the nation's security, including but not limited to, positions requiring eligibility for access to Top Secret or DOE "Q" level classified information, positions involving development or approval of war plans, major or special operations of war, or critical and extremely important items of war, national security policy-making or policy-determining positions, the duties of which have the potential to cause exceptionally grave damage to the national security, positions involving investigative duties, including handling of CI investigations or background investigations, the nature of which has the potential to cause exceptionally grave damage to the national security. Fiduciary duties: Duties that involve the obligation, expenditure, collection, or control of revenue, funds, or items with value over $50 million dollars, or procurement or securing funding for goods or services with monetary value in excess of $50 million dollars annually.

Noncritical-Sensitive

Noncritical-sensitive positions can cause significant damage to national security, including positions requiring eligibility for access to Confidential, Secret, or DOE "L" level information, positions not requiring eligibility for access to classified information, but having potential to cause significant or serious damage, positions requiring access to automated systems that contain military active duty, guard, or reservists' personally identifiable information, and positions designated by the DoD Component head.

Nonsensitive

If a position does not meet the criteria for any of the other position sensitivity levels, it is designated nonsensitive. Nonsensitive positions do not require access to classified information or performance of national security sensitive duties. These positions pose no potentially adverse effects on national security.

Mixed-Civilian Designations

A mixed-civilian designation is a position involving job duties with different levels of impact on the national security. Mixed duties involve any level of sensitive and/or non-sensitive or critical-sensitive and/or noncritical-sensitive duties. Where someone has a mix of duties, the highest level of duty determines the sensitivity.

Military/Contractor Designations

Military and contractor personnel have designations distinct from civilian employees. Both military and contractor personnel are granted eligibility to access classified information and perform national security sensitive duties comparable to civilians.

Other Designations

Only U.S. citizens are eligible for access to classified information. However, when compelling reasons exist, non-U.S. citizens who require classified access to perform official duties can be granted a Limited Access Authorization. For example, a non-U.S. citizen who has special expertise or knowledge may receive an LAA. An LAA enables a non-U.S. citizen to have limited access to classified information, but the LAA is not a national security eligibility. Additionally, all LAAs are required to be reviewed annually to determine if continued access is in compliance with DoD policy. The investigative requirement for an LAA is a Tier 5 national security investigation. An LAA can be granted to civilian, military, or contractor personnel.

Special Access Programs

There are some special requirements for access to information related to programs that impose access controls beyond those normally provided for Confidential, Secret, or Top Secret information. Special programs provide an additional layer of security to some of our nation's most sensitive assets.

When an individual's work involves access to such information, he or she requires a more extensive national security background investigation and adjudication, with additional questions asked of personal sources prior to an eligibility determination.

Special programs cover a variety of areas, including Presidential support activities, Yankee White; special access programs; NATO; Nuclear Personnel Reliability Program also known as Nuclear PRP; Sensitive Compartmented Information also known as SCI; Nuclear Command and Control – Extremely Sensitive Information or NC2-ESI; and Chemical PRP.

The Nuclear Personnel Reliability Program, or Nuclear PRP, functions to ensure that each person performing duties associated with nuclear weapons or nuclear command and control systems and equipment is not only emotionally stable and physically capable, but also demonstrates reliability and professional competence.

In addition to the specific categories of information covered by Special Access Programs, there are special requirements for access and dissemination of Restricted Data and Critical Nuclear Weapon Design Information, or CNWDI.

Restricted Data includes all information concerning the design, manufacturing, or use of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy. Restricted Data is not a Special Access Program nor is it a classification category. Rather, it is an additional warning notice of special handling requirements.

CNWDI is Restricted Data classified as Top Secret or Secret. It includes information about operational theory or design components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition, or test device.

Knowledge Check

Question 1 of 3
Joe Smith is a Division Chief who works at a DoD agency. He has a mix of civilians, military service members, and contractors working for him who have different national security eligibility and access levels.

The majority of Joe's employees are civilians who work on projects that require access to Top Secret information. Which of the following categories describes these civilian employee positions?

- Noncritical-sensitive
- Critical-sensitive
- Special-sensitive

Question 2 of 3
Joe also has an individual on temporary assignment working in his office. He is a member of the Canadian Air Force. The officer has unusual expertise and knowledge for a position that a U.S. citizen does not have. To be eligible to do the job, the officer receives which of the following?

- Access
- National security eligibility
- Limited Access Authorization

Question 3 of 3

Special access requirements are designed to provide an additional layer of security to some of our nation's most valuable assets.

- True
- False

Answers

Question 1 of 3
Joe Smith is a Division Chief who works at a DoD agency. He has a mix of civilians, military service members, and contractors working for him who have different national security eligibility and access levels.

The majority of Joe's employees are civilians who work on projects that require access to Top Secret information. Which of the following categories describes these civilian employee positions?

- Noncritical-sensitive
- **Critical-sensitive**
- Special-sensitive

Question 2 of 3
Joe also has an individual on temporary assignment working in his office. He is a member of the Canadian Air Force. The officer has unusual expertise and knowledge for a position that a U.S. citizen does not have. To be eligible to do the job, the officer receives which of the following?

- Access
- National security eligibility
- **Limited Access Authorization**

Question 3 of 3
Special access requirements are designed to provide an additional layer of security to some of our nation's most valuable assets.

- **True**
- False

Position Designation and Special Access Requirements Summary

This lesson explained who could obtain access to classified information and what the requirements are to make that happen. It also covered how designations and access programs to build a foundation for what is ahead as you learn more about the PSP.

Lesson 4: Investigation and Adjudication

This lesson will cover the roles and responsibilities of a security specialist, security reporting requirements, and required security briefings.

Lesson Objectives:

- Identify roles and responsibilities of a security specialist
- Determine security reporting requirements
- Explain required security briefings

Investigation and Adjudication

This lesson covers the national security eligibility process, requirements for "other" types of access, Federal Investigative Standards, or FIS, and the adjudicative guidelines.

What is National Security Eligibility?

National security eligibility is a favorable determination that affords an individual eligibility for access to classified information or assignment to a national security sensitive position.
Even when national security eligibility is established, it does not guarantee access to classified information. Access determinations are made solely on the basis of the eligible individual's need for access to classified information to perform official duties. The employing activity determines access level based on eligibility, need-to-know, and the requirements of the position held.

It's necessary to complete an assessment of an individual's specific situation and/or position and to determine what regular access means in order to establish the need for national security eligibility. For example, the Department of Defense does not define regular access in terms of specific time. Regular access might mean daily, weekly, or even monthly access, depending on a specific defense organization's access controls.

Initiating the National Security Eligibility Process

Granting national security eligibility is a four-phased process. An authorized agency initiates a request for a national security eligibility determination for an individual. An Investigative Service Provider, or ISP, moves forward to conduct a background investigation to provide required information. Once an individual's PSI is completed, the ISP will use centralized databases to send the results to the Department of Defense Consolidated Adjudications Facility, or CAF, for a determination. CAF reviews the information in PSI and compares it to national adjudication standards. Based on the information provided in the PSI, the CAF makes a determination and either grants or denies national security eligibility.

Limitations and Restrictions

There are limitations and restrictions for submitting investigations. Personnel who are employed by or serving in a military, civilian, contractor, or consultant capacity may be considered for

national security eligibility only when such eligibility is required for a lawful and authorized government purpose in connection with official duties.

To conserve investigative resources and prevent unnecessary investigations, guidelines have been established for requesting a national security background investigation. These guidelines include limiting national security investigation requests to only those personnel who are essential to current operations; limiting investigation requests for military personnel to those individuals with sufficient time left in the service to warrant conducting the investigation; properly completing all requested forms and required documentation in accordance with instructions; submitting Government personnel requests through e-QIP to their respective Investigative Service Provider; submitting industry requests through the Vetting Risk Operations Center or VROC; limiting access through strict need-to-know; and keeping priority case requests to a minimum.

There are also restrictions to national security eligibility. Non-U.S. citizens, civilians in nonsensitive positions, individuals who may have had inadvertent access or exposure to sensitive or classified information, and individuals who would require eligibility only for "ease of movement" are included among the categories of restricted eligibility.

Adjudication

The adjudicative process begins once a personnel security investigation is completed by the ISP and sent to the CAF for an eligibility determination. The adjudicative process is an examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. This is known as the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a national security eligibility determination.

Eligibility

Once an individual’s PSI is complete, adjudicators consider all the collected information to determine his or her eligibility. Eligibility could be access to classified information or assignment to a national security sensitive position.

Personal information is collected in several different ways. They include having the person fill out forms, respond to questions in writing, or speak directly with an investigator.

Investigators may also obtain releases from the individual for access to personal, medical, and financial information. They may investigate court records, interview personal references, or other sources. In certain circumstances, they may conduct a polygraph when required, which carries some restrictions.

The national security eligibility process begins when a person completes a security questionnaire. The questionnaire used for this purpose is the Questionnaire for National Security Positions, or SF-86. Included in this standard form are releases that the subject must sign to

enable the investigator to obtain record information and/or interview references. After the background investigation is completed, a report is submitted for subsequent adjudication. The report includes information from many different personal sources and records that give adjudicators a comprehensive view of the individual. This allows the adjudicators to make a sound determination regarding a person's national security eligibility.

Need-to-Know

Having a national security eligibility does not give one open, unfettered access to classified information. As a security specialist, you will often hear and use the term "need-to-know."

Before an individual receives access to any classified information, he or she must have national security eligibility for that level of information, have signed the Classified Information Nondisclosure Agreement, Standard Form 312 or SF-312, and have an official need-to-know.

As a security specialist, you are responsible for making sure that people adhere to access rules in the interest of protecting classified information.

Reciprocity

Each agency that grants its employees access to classified information is responsible for determining whether these employees were previously cleared or investigated by the Federal Government. Unauthorized, unnecessary, or duplicative PSIs are prohibited. An investigation will not be requested when there is no requirement.

E.O. 13467 establishes the DNI as the SecEA responsible for ensuring reciprocal recognition of national security eligibility among the agencies. All federal agencies should reciprocally accept existing national security eligibility determinations or national security eligibilities from other government agencies in accordance with E.O. 13467, regardless of which agency issued the determination, as long as it meets or exceeds the suitability requirements of the new position.

Reciprocity refers to the mutual acceptance of a national security eligibility by all government agencies, regardless of which agency issued the national security eligibility. DoD 5220.22-M the National Industrial Security Program Operating Manual, better known as the NISPOM, addresses reciprocity for government contractors. The NISPOM advises that it is the contract company's responsibility to refrain from initiating a new background investigation on the behalf of a government agency if an employee applicant already has the appropriate national security eligibility or is in the process for the same clearance eligibility by another agency.

Whether working for the government or for a contractor, a previously eligible individual is not subject to a new investigation or adjudication unless the previous national security eligibility was based on an outdated investigation, new derogatory information has become available since the previous investigation, there was a break of more than 24 months in the individual's relationship with the DoD, or the previous investigation does not meet the scope required for this sensitive position.

National Security Databases

Now that you are familiar with the background investigative process, I would like for you to start familiarizing yourself with the personnel security databases. Become familiar with these databases: e-QIP, JPAS, DISS, SWFT and NBIS.

National Security Databases – e-QIP

To start the national security eligibility process, an official of an authorized agency must initiate the investigation using the Electronic Questionnaires for Investigations Processing, or e-QIP.

e-QIP is a web-based automated database designed to facilitate the processing of standard investigative forms used when conducting background investigations for federal security, suitability, fitness, and credentialing purposes. It allows applicants to electronically enter, update, and transmit their personal investigative data over a secure internet connection to an Investigative Service Provider, or ISP.

Different kinds of adjudications have different investigative requirements and therefore utilize different e-QIP forms. National Security Adjudications, which grant access eligibility for SCI, Top Secret, Secret, or Confidential information, or assignment to a national security sensitive position, require an SF-86.

It is important to note that non-national security adjudications, such as suitability for federal employment, require different forms depending upon the position. Nonsensitive high-risk public trust positions and moderate-risk public trust positions require an SF-85P, while nonsensitive low-risk positions and basic suitability require an SF-85. The SF-85 is also required for individuals needing physical access to government-controlled facilities or logical access to government information systems.

Note, however, that if an individual fits more than one of these categories, the highest responsibility always applies. For example, if an individual needs Secret access eligibility and will also hold a moderate-risk public trust position, he or she will only need to fill out an SF-86.

National Security Databases – JPAS

The Joint Personnel Adjudication System, or JPAS, is currently the centralized database for DoD adjudicative actions and determinations. JPAS is the DoD system that connects security personnel around the world with a database managed by Defense Manpower Data Center (DMDC).

National Security Databases – DISS

Defense Information System for Security (DISS), which is currently deployed in phases, will ultimately replace JPAS. DISS was established to specifically address the national security eligibility and suitability determination requirements outlined in the Intelligence Reform and Terrorism Prevention Act of 2004, IRTPA, as well as to support Homeland Security Presidential

Directive 12, or HSPD-12 compliance across DoD.

DISS is a secure, end-to-end Information Technology system that reduces the DoD personnel national security eligibility, suitability, and HSPD-12 process cycle times by electronically collecting, reviewing, and sharing relevant data among appropriate government agencies.

DISS is an Enterprise capability that includes the Joint Verification System, or JVS, Reporting, Service Desk, and Appeals. Together, these systems replace JPAS and manage the adjudication process for national security eligibility as well as HSPD-12 and suitability determinations for all DoD employees, military personnel, civilians, and contractors. JVS provides DoD Security Managers and Officers with current eligibility information and the ability to update personnel security information and security history.

National Security Databases – SWFT

The Secure Web Fingerprint Transmission (SWFT) secure electronic system captures and submits fingerprint images in support of the national security background investigation process. SWFT expedites the process and provides end-to-end accountability for personally identifiable information.

National Security Databases – NBIS

The National Background Investigation System (NBIS) is a federal-wide information technology service. The NBIS is used to conduct suitability, security, and will house all systems-identified data associated with credentialing investigations for all Federal civilians, military service members, and government contractors. The system will protect the sensitive information used to adjudicate investigations by employing the latest modern technology and utilizing maximum security resources to guard against increasingly sophisticated and evolving threats by leveraging DoD's national security, IT, and cybersecurity expertise.

Interim Eligibility

Unless otherwise prohibited by policy, an individual may be granted temporary national security eligibility pending investigation and a final determination when his or her official functions must be performed before completion of the investigation and adjudication process.

Interim eligibility allows employees to begin working on sensitive or classified projects while awaiting final determination for a national security eligibility by the adjudication facility. Only government personnel may make interim determinations. Justification for interim eligibility will be recorded in the system of record and the employee must be notified in writing by their employing activity that further access is expressly conditioned upon the completion of the national security investigation and granting of national security eligibility.

Not all employees are eligible for interim eligibility. Prior to granting interim eligibility, organizations must ensure that the individual has submitted a favorably reviewed SF-86 and the ISP must have opened the proper investigation. Interim eligibility is valid for up to one year but

may be extended for an additional six months by the designated component authority under certain conditions.

Interim Eligibility Requirements

Minimum requirements for interim Top Secret eligibility are a favorable completion of all requirements cited for interim Secret or Confidential eligibility and favorable completion of a National Agency Check.

One-time Access

Circumstances may arise where an urgent operational or contractual need exists for cleared DoD personnel to have one-time or short-duration access to classified information at a higher level than authorized by the existing eligibility level. One-time access allows personnel to access higher-level information without a full security upgrade.

When the processing time required to upgrade the eligibility would preclude timely access to the information the DoD may grant one-time access to personnel with an existing eligibility who need short-term access to classified information at a higher level than they are currently authorized.

It might happen if a person has Secret eligibility but needs access to Top Secret information due to an urgent operational or contractual situation. However, this is quite rare and the exercise of this provision will be used sparingly. Repeatedly issuing multiple short duration accesses for the same individual during any 12-month period is prohibited.

Federal Investigation Standards

As you can see, we handle many interim eligibilities here. It is important that we ensure requirements for interim and one-time access are met. But what are the standards that we must follow?
Well, that leads to our next training topic, Federal Investigative Standards.

The Federal Investigative Standards, also known as FIS, is a five-tiered investigative model developed in accordance with Executive Order 13467. The FIS sets standard requirements used to conduct background investigations that determine eligibility to access classified information or hold a national security sensitive position. It decides suitability or fitness for Federal Government employment and eligibility for logical and physical access to Federal Government-controlled facilities and information systems for HSPD-12 credentialing.

The five-tiered model facilitates reciprocity, uses a build-upon, but not duplicative investigative principle, and facilitates the use of automation. Each successively higher level of investigation builds upon the levels below. In its investigations, the FIS also establishes an Expandable Focused Investigative model.

At each tier, if the standard investigation flags a potential issue, an Expandable Focused Investigation, or EFI will be conducted to develop and resolve any pertinent issues.

<table>
<tr><td rowspan="2">HSPD-12</td><td rowspan="2">Suitability</td><td>National Security</td></tr>
<tr><td>Classified information and/or sensitive positions</td></tr>
<tr><td></td><td>Suitability for federal employment</td><td></td></tr>
<tr><td>Logical and/or physical access</td><td>Fitness for federal contractors</td><td rowspan="2">Tier 5</td></tr>
<tr><td rowspan="3"></td><td>Tier 4</td></tr>
<tr><td rowspan="2">Tier 3</td></tr>
<tr><td>Tier 2</td></tr>
<tr><td colspan="2">Tier 1</td></tr>
</table>

Federal Investigation Standards - Tiers

The FIS is a five-tiered investigative model that replaces several investigations that were previously used to grant national security eligibility. Let's review details for each of the tiers.

- **Federal Investigation Standards – Tier 1**

  Tier 1 investigations are conducted for positions designated as low-risk, nonsensitive, and for physical and logical access; that is, HSPD-12 credentialing. The investigative form is Standard Form, SF-85. Tier 1 investigations replace the National Agency Check with Inquiries, or NACI.

  The NACI was an initial investigation used for basic suitability and HSPD-12 credentialing determinations. Tier 1 investigations have a basic scope of five years.

- **Federal Investigation Standards – Tier 2**

  Tier 2 investigations are conducted for positions designated as nonsensitive, moderate-risk public trust. The investigative form is Standard Form, SF-85P. Tier 2 replaces the Moderate-Risk Background Investigation, or MBI.

  The MBI was used to assess nonsensitive, moderate-risk public trust positions that did not grant access to classified information. Tier 2 investigations have a basic scope of five years.

- **Federal Investigation Standards – Tier 3**

Tier 3 investigations are conducted for positions designated as noncritical-sensitive, and/or requiring Confidential, Secret or DOE " L " access eligibility and military accessions. The investigative form is SF-86.

Tier 3 investigations replace the National Agency Check with Law and Credit, or NACLC, which was formerly used to grant initial Secret and Confidential national security eligibility to military and contractor personnel. Tier 3 investigations also replace the Access National Agency Check with Inquires, or ANACI, used to grant initial Secret and Confidential eligibility for civilians. Tier 3 investigations have a basic scope of five years.

- **Federal Investigation Standards – Tier 4**

  Tier 4 investigations are conducted for positions designated as nonsensitive, high-risk public trust. The investigative form is SF-85P. Tier 4 replaces the Background Investigation, or BI, which was used for nonsensitive, high-risk public trust positions.

  Tier 4 investigations have a basic scope of five to seven years.

- **Federal Investigation Standards – Tier 5**

  Tier 5 investigations are conducted for positions designated as critical-sensitive or special-sensitive and/or requiring DOE "Q" access or access to Top Secret or Sensitive Compartmented Information, or SCI. The investigative form is SF-86.

  Tier 5 investigations replace the Single Scope Background Investigation, or SSBI, which was previously used to grant Top Secret or SCI eligibility. Tier 5 investigations have a basic scope of five to seven years.

Knowledge Check

Question 1 of 4

_____ The DoD CAF makes a determination to grant or deny national security eligibility.
_____ A security office initiates the investigation and forwards to an ISP to start the background investigation.
_____ The ISP forwards the investigation results to the DoD CAF.
_____ The DoD CAF reviews the information in the investigation and provides a determination using 13 national security adjudicative guidelines.

A. Step 1
B. Step 2
C. Step 3
D. Step 4

Question 2 of 4
Which of the following may prevent an individual from receiving national security eligibility?

- You are not a U.S. Citizen
- Your position is nonsensitive
- You received an unfavorable adjudication determination
- All of the above

Question 3 of 4
Which level of investigation would someone need to receive eligibility to access Top Secret information?

- Tier 2
- Tier 3
- Tier 4
- Tier 5

Question 4 of 4
Which level investigation would a person need if their position only required eligibility for Confidential access?

- Tier 2
- Tier 3
- Tier 4
- Tier 5

Answers

Question 1 of 4
_____ The DoD CAF makes a determination to grant or deny national security eligibility.
_____ A security office initiates the investigation and forwards to an ISP to start the background investigation.
_____ The ISP forwards the investigation results to the DoD CAF.
_____ The DoD CAF reviews the information in the investigation and provides a determination using 13 national security adjudicative guidelines.

E. Step 1
F. Step 2
G. Step 3
H. Step 4
Answer: D, A, B, C

Knowledge Check 2
Which of the following may prevent an individual from receiving national security eligibility?

- You are not a U.S. Citizen
- Your position is nonsensitive
- You received an unfavorable adjudication determination
- **All of the above**

Knowledge Check 3
Which level of investigation would someone need to receive eligibility to access Top Secret information?

- Tier 2
- Tier 3
- Tier 4
- **Tier 5**

Knowledge Check 4
Which level investigation would a person need if their position only required eligibility for Confidential access?

- Tier 2
- **Tier 3**
- Tier 4
- Tier 5

Investigation and Adjudication Summary

This lesson discussed the national security eligibility process, requirements for "other" types of access, Federal Investigative Standards, or FIS, and the adjudicative guidelines.

Lesson 5: Investigative Service Providers and Record Keeping

An Investigative Service Provider, or ISP, conducts a background investigation to provide required information. The ISP forwards completed investigations to the Department of Defense Consolidated Adjudications Facility, or CAF, and other federal agencies.

The final consideration in the national security background investigation process is how to handle and store personnel records. Let's look at responsibilities for handling and storing records.

Lesson Objectives:

- Understand who has access to and responsibility for Investigation Records
- Identify the details for disposing and destroying Investigation Records
- Describe the Adjudicative Process and the National Adjudicative Guidelines

Responsibility for Investigation Records

The responsibility for safeguarding background investigation records rests with the DoD authorities who administer the DoD PSP and all authorized DoD personnel who have access to such records. To make certain that background investigation information is used only for official and authorized purposes, DoD components must have a system in place of internal controls to protect records from unauthorized access or disclosure and to preserve confidentiality.

There are several procedures to safeguard background investigative reports and other personnel security records. First, authorized requesters are responsible for control and accountability of any reports they receive. Second, rules restrict reproduction of background investigation reports to a minimum number of copies required to perform official duties. Third, background investigation reports must be stored in a secured container, such as a vault or safe. Fourth, background investigation reports must be sealed in double envelopes when being transmitted by mail or courier. Finally, any personal information regarding an individual's national security eligibility status must be protected.

Access to Investigation Records

To protect the fundamental right to privacy of individuals under investigation, rules limit access to background investigation records and information to only those whose official duties require access to such information. Background investigation reports may be released outside of the DoD only with the specific approval of the investigative agency with authority over the reports. Within the DoD, only designated DoD officials who require access for official personnel security duties may have access to background investigation reports. Subjects of background investigations may also have access to background investigation information. Specifically, they have the right to determine what records exist pertaining to them; they have the right to gain access to such records; and they have the right to correct or amend such records.
Rules restrict information about personnel national security eligibility determinations to designated DoD or other Federal Government officials who require access for official personnel security duties and who have an official need-to-know.

Disposition and Destruction of Investigation Records

Strict regulations describe how to dispose and destroy background investigation records. DoD recipient organizations requesting background investigation records may retain them for only the time necessary to fulfill the originally requested official purpose. These records are the property of the investigating organization and are only on loan when received by a requesting organization.

Only specially authorized DoD records depositories store background investigation records. Favorable records are destroyed after 15 years. The same is true of records of a minor derogatory nature. However, records resulting in unfavorable administrative action or court-martial wait for 25 years before destruction. Finally, background investigations existing on individuals who were considered for DoD affiliation but never completed their affiliation are destroyed after one year.

The Adjudication Process

Now that you understand the investigation process, let's move on to adjudication. You will have a brief overview of the adjudicative process this week.

Adjudicators utilize all available, reliable information about a person — past and present, favorable, and unfavorable — to make an adjudicative determination for national security eligibility. Sources of information include Reports of Investigation (ROI), credit reports, and other agency checks. The 13 National Security Adjudicative Guidelines are applied against this information.

Several intelligence agencies and other organizations, in addition to granting security eligibility determinations, also make decisions regarding special access eligibility for employees whose duties involve exceptionally sensitive information. The Director of National Intelligence, or DNI, Security Executive Agent Directive 4, or SEAD 4, National Security Adjudicative Guidelines, provides guidelines for determining eligibility for access to classified information or assignment to sensitive duties.

Ultimately, national security eligibility must be consistent. The decision to grant or continue eligibility must be an overall common sense determination based upon careful consideration of the whole person concept that is reflected by 13 National Security Adjudicative Guidelines. The 13 National Security Adjudicative Guidelines are Allegiance to the United States, Foreign Influence, Foreign Preference, Sexual Behavior, Personal Conduct, Financial Considerations, Alcohol Consumption, Drug Involvement and Substance Misuse, Psychological Conditions, Criminal Conduct, Handling Protected Information, Outside Activities, and Use of Information Technology.

National Security Adjudicative Guidelines

Each of the 13 National Security Adjudicative Guidelines identifies a potential security concern that may have an adverse impact on national security. Some guidelines deal with cases in which a subject's loyalty to the U.S. may be in question. These include: Guideline A: Allegiance to the

U.S.; Guideline B: Foreign Influence; Guideline C: Foreign Preference.

There are guidelines that deal with cases in which the subject's reliability, trustworthiness, and ability to protect classified information enter into question. These include: Guideline D: Sexual Behavior; Guideline E: Personal Conduct; Guideline F: Financial Considerations.
Other guidelines deal with medical issues that might influence an individual's ability to protect classified information. These include: Guideline G: Alcohol Consumption; Guideline H: Drug Involvement and Substance Misuse; Guideline I: Psychological Conditions.

Finally, some guidelines cover illegal and other noncompliant behaviors. These include: Guideline J: Criminal Conduct; Guideline K: Handling Protected Information; Guideline L: Outside Activities; Guideline M: Use of Information Technology.

As you become a more experienced security specialist, you will need to become more familiar with components of each guideline. Each specific guideline carries with it three components. SEAD 4, Appendix A describes them as: The Concern; Conditions that could raise a security concern and may be disqualifying; Conditions that could mitigate security concerns.

Knowledge Check

Question 1 of 3
Facts: Jim Johnson, a newly assigned civilian employee, requires Top Secret eligibility. During his background investigation, an investigator interviewed Mr. Johnson and learned that, when he was in college, Mr. Johnson was the secretary of the New Free America Liberation Coalition. This group's goal is to overthrow the U.S. government and establish a worker state. This group seeks to achieve its goal through any means, including violence.

While Mr. Johnson supported the concept of a worker state, he thought it would come about through the election process. When he learned the full extent of the group's goals, he left the organization. The investigator confirmed this through interviews with developed or listed references. In addition, Mr. Johnson's completed investigation contains a statement about his current intention to support the U.S. government.

Which National Security Adjudicative Guideline would adjudicators use to determine Jim's eligibility?

- Guideline A: Allegiance to the United States
- Guideline E: Personal Conduct
- Guideline K: Handling Protected Information
- Guideline D: Sexual Behavior

Question 2 of 3
Facts: John Lewis was born in the United States to British citizens who were legally residing and working in the United States at the time of his birth. He acquired British citizenship through his parents and has a current British passport. He is applying for a position in the U.S. government that requires Top Secret eligibility. As required, he disclosed his foreign citizenship and passport

on his security form.

He has never had access to classified information or held a national security sensitive position. During the interview portion of his investigation, Mr. Lewis disclosed that even though he was born in the United States, he holds British citizenship through his parents and maintains a British passport. He advised he only uses his U.S. passport when traveling to and from the United States. He also stated that he does not exercise any rights, privileges, or obligations associated with his foreign citizenship and does not hold any foreign financial or business interests.

Which National Security Adjudicative Guideline would be a concern when adjudicators determine John's eligibility?

- Guideline A: Allegiance to the United States
- Guideline I: Psychological Conditions
- Guideline C: Foreign Preference
- Guideline J: Criminal Conduct

Question 3 of 3
Facts: Annie Wheaton is a contract employee who requires Top Secret eligibility to perform on a DoD contract. During the interview portion of the investigation, Ms. Wheaton told the investigator that she enrolled in an alcohol treatment program five years ago, after suffering a blackout.

She learned she has an alcohol use disorder. She was required to complete inpatient counseling and meet aftercare requirements. Ms. Wheaton completed the inpatient counseling and enrolled in Alcoholics Anonymous as an aftercare program. She acknowledged that she now controls her drinking and consumes alcohol only on holidays and special occasions.

Which National Security Adjudication Guidelines would adjudicators use to determine Annie's eligibility?

- Guideline C: Foreign Preference
- Guideline G: Alcohol Consumption
- Guideline I: Psychological Conditions
- Guideline J: Criminal Conduct

Answers

Question 1 of 3
Facts: Jim Johnson, a newly assigned civilian employee, requires Top Secret eligibility. During his background investigation, an investigator interviewed Mr. Johnson and learned that, when he was in college, Mr. Johnson was the secretary of the New Free America Liberation Coalition. This group's goal is to overthrow the U.S. government and establish a worker state. This group seeks to achieve its goal through any means, including violence.

While Mr. Johnson supported the concept of a worker state, he thought it would come about through the election process. When he learned the full extent of the group's goals, he left the organization. The investigator confirmed this through interviews with developed or listed references. In addition, Mr. Johnson's completed investigation contains a statement about his current intention to support the U.S. government.

Which National Security Adjudicative Guideline would adjudicators use to determine Jim's eligibility?

- **Guideline A: Allegiance to the United States**
- Guideline E: Personal Conduct
- Guideline K: Handling Protected Information
- Guideline D: Sexual Behavior

Question 2 of 3
Facts: John Lewis was born in the United States to British citizens who were legally residing and working in the United States at the time of his birth. He acquired British citizenship through his parents and has a current British passport. He is applying for a position in the U.S. government that requires Top Secret eligibility. As required, he disclosed his foreign citizenship and passport on his security form.

He has never had access to classified information or held a national security sensitive position. During the interview portion of his investigation, Mr. Lewis disclosed that even though he was born in the United States, he holds British citizenship through his parents and maintains a British passport. He advised he only uses his U.S. passport when traveling to and from the United States. He also stated that he does not exercise any rights, privileges, or obligations associated with his foreign citizenship and does not hold any foreign financial or business interests.

Which National Security Adjudicative Guideline would be a concern when adjudicators determine John's eligibility?

- Guideline A: Allegiance to the United States
- Guideline I: Psychological Conditions
- **Guideline C: Foreign Preference**
- Guideline J: Criminal Conduct

Question 3 of 3

Facts: Annie Wheaton is a contract employee who requires Top Secret eligibility to perform on a DoD contract. During the interview portion of the investigation, Ms. Wheaton told the investigator that she enrolled in an alcohol treatment program five years ago, after suffering a blackout.

She learned she has an alcohol use disorder. She was required to complete inpatient counseling and meet aftercare requirements. Ms. Wheaton completed the inpatient counseling and enrolled in Alcoholics Anonymous as an aftercare program. She acknowledged that she now controls her drinking and consumes alcohol only on holidays and special occasions.

Which National Security Adjudication Guidelines would adjudicators use to determine Annie's eligibility?

- Guideline C: Foreign Preference
- **Guideline G: Alcohol Consumption**
- Guideline I: Psychological Conditions
- Guideline J: Criminal Conduct

Investigative Service Providers and Record Keeping Summary

- This lesson covered who has access to and responsibility for Investigation Records, the details for disposing and destroying Investigation Records, and the Adjudicative Process and the National Adjudicative Guidelines.

Lesson 6: Continuous Evaluation and Reinvestigation

There is a clear need to assure the ongoing trustworthiness of an individual, even after reaching an initial personnel security determination. The need is met by a "Continuous Evaluation" process that reviews the background of an individual who has been determined to be eligible for access to classified information or who holds a sensitive position at any time during the period of eligibility.

Known as CE, it supplements but does not replace, scheduled periodic reinvestigations. The organization's manager, supervisor, co-worker, AND the individual share the responsibility to satisfy this process.

It's important to have close coordination between law enforcement, personnel, medical, legal, and supervisory personnel to consider all pertinent information under the personnel security process.

All individuals who hold national security eligibility are subject to continuous evaluation. Let's go over some additional information.

Lesson Objectives:

- Recognize the need for continuous evaluation and reinvestigation
- Examine who is responsible for the continuous evaluation and reinvestigations
- Determine the issues of concern in the continuous evaluation process

Purpose

It is the responsibility of all security personnel to continuously evaluate personnel assigned to their organization or activity.

Anyone who becomes aware of information that might make an individual ineligible for a national security eligibility must report this information to his or her supervisor or to a local security official.

Periodic reinvestigations take place as part of the process of continuous evaluation. In the near future, continuous evaluation will incorporate an automated record check monitoring system to cover the gap between initial and periodic reinvestigations.

Supervisors, coworkers, and individuals themselves all have an obligation to report potentially disqualifying information.

Continuous Evaluation Requirements

Behaviors that could cause a security concern and that should be reported are: a crime that will be reported to a law enforcement authority; an incident or behavior that will be reported to the Military Department CI Organization in accordance with DoDD 5240.06; Information that

suggests an individual may have an emotional, mental, or personality condition that can impair judgment, reliability, or trustworthiness will be reported to the supporting adjudication facility.

Individuals who have been granted national security eligibility should recognize and avoid the kind of personal behaviors that would render them ineligible for continued access to classified information or assignment to sensitive positions.

In the final analysis, the ultimate responsibility for maintaining continued national security eligibility rests with the individuals.

Examples of Information may include, but is not limited to:

- A known history of a mental disorder
- A report that an individual has sought treatment for a mental, emotional, or substance abuse condition (commensurate with any reporting limitations of Section 21 on the SF-86)
- Direct and indirect threats of violence
- Physical altercations, assaults, or significant destruction of U.S. Government property
- An abrupt and significant change in an individual's appearance or behavior suggesting impaired judgement or stability (e.g., deteriorating physical appearance or self-care, social withdrawal)
- Signs of substance use or intoxication on the job
- An indication of substance abuse after completion of treatment
- Evidence of alcohol or drug related behavior outside the workplace (e.g., driving under the influence, public intoxication charges)
    - Suicide threats, attempts, or gestures or actions
    - Any other behaviors that appear to be abnormal and indicate impaired judgement, reliability, or maturity

CE Supervisor Responsibilities

Supervisors, security specialists, and individuals all have responsibilities for continuous evaluation.

Supervisors will continuously evaluate individuals with national security eligibility to determine if they continue to be trustworthy in accordance with the security guidelines in the 2017 National Security Adjudicative Guidelines.

Report any derogatory information that falls within the adjudicative guidelines, such as government travel card misuse, abuse, or fraud, to their cognizant security specialist or supervisor. Failure to report derogatory information may trigger an adverse security action.

Ensure the discharge of security responsibilities is included in personnel performance evaluations.

CE Employee Responsibilities

Personnel should become familiar with pertinent security regulations that pertain to their assigned duties. It is their obligation to be aware of the standards of conduct and the security requirements of persons who have received national security eligibility. Personnel should recognize and avoid the kind of personal behavior that would render them ineligible for continued eligibility to access classified information or assignment to sensitive positions.

In the final analysis, the ultimate responsibility for maintaining continued national security eligibility rests with the individuals. Personnel having access to classified information will protect classified information in their custody from unauthorized disclosure and be aware of and comply with periodic reinvestigations (PR), CE, and reporting requirements.

CE Issues and Reporting

You should consider reporting these behaviors if you observe them, so that your supervisor or the security office can determine whether some type of preventive or investigative action is appropriate. If ignored, problems signaled by the behaviors listed in this job aid could cause significant problems. Such behaviors may impair the health, well-being, or performance of the individual employee, disrupt the work unit, or lead to compromise of sensitive information. Security judgments are based upon a pattern of behavior, and not a single action. It is a whole person judgment that takes many factors into account, including strengths as well as weaknesses.

Periodic Reinvestigation Requirements

Can you see how continuous evaluations incorporate the requirement for periodic reinvestigations?

In accordance with FIS, reinvestigations may be performed at any time after national security eligibility has been granted. Additionally, DoD employees in national security positions and contractor personnel performing national security duties will be subject to periodic reinvestigation (PR) on a recurring basis. Submission of out-of-scope reinvestigations must be justified before approval of the submission.

Submit PR requests no earlier than three months before the respective anniversary date of the close date of the last investigation. Military and civilian personnel for whom periodic investigation requests are initiated must have at least 12 months remaining in service or employment. Make every effort to ensure PRs are conducted within the current prescribed timeframes so as not to undermine the ability of the DoD to accomplish its mission.

A national security eligibility determination is current if the reinvestigation is submitted to the investigation service provider within five years of the previous investigation close date. Personnel assigned to a North Atlantic Treaty Organization, or NATO, staff position may submit a reinvestigation request up to one year in advance of the required timeframe.

FIS Tier 3 and Tier 5 investigations are used to make initial national security eligibility determinations. Periodic reinvestigations will be required at least every five years for Tiers 2 and 5.

The Tier 3 Reinvestigation, or T3R, is the periodic reinvestigation required for military, civilian, and contractor personnel for continued Confidential, Secret, or DOE "L" access eligibility, and for those civilian personnel occupying noncritical-sensitive positions. The reinvestigation initiates no later than 5 years from the close of the previous investigation.

The Tier 5 Reinvestigation, or T5R, is the periodic reinvestigation for continued Top Secret, SCI, or DOE "Q" access eligibility and for other positions that required a Tier 5 investigation. Each DoD military and civilian employee occupying a special-sensitive or critical-sensitive position and each contractor personnel requiring continuing national security eligibility at an equivalent level will undergo a reinvestigation initiated on a 5-year recurring basis.

Per DNI Memorandums dated Feb 16, 2017 and Feb 27, 2019, the DoD will delay the 5-year reinvestigation cycle for Tier 3 and increase the Tier 5 reinvestigation timeline to six years until further notice.

Knowledge Check

Question 1 of 4
The purpose of continuous evaluation is to identify potential issues that could affect an individual's national security eligibility.

- True
- False

Question 2 of 4
The continuous evaluation process is the uninterrupted assessment of an individual for the retention of a job.

- True
- False

Question 3 of 4
Information about an individual who has national security eligibility is monitored continuously.

- True
- False

Question 4 of 4
Once a person receives national security eligibility, they are no longer subject to an investigation.

- True
- False

Answers

Question 1 of 4
The purpose of continuous evaluation is to identify potential issues that could affect an individual's national security eligibility.

- **True**
- False

Question 2 of 4
The continuous evaluation process is the uninterrupted assessment of an individual for the retention of a job.

- True
- **False**

Question 3 of 4
Information about an individual who has national security eligibility is monitored continuously.

- **True**
- False

Question 4 of 4
Once a person receives national security eligibility, they are no longer subject to an investigation.

- True
- **False**

Continuous Evaluation and Reinvestigation Summary

This lesson discussed the need for continuous evaluation and reinvestigations, who is responsible for CE and reinvestigations, and issues of concern in the CE process.

Lesson 7: The Security Specialist

This lesson will help in identifying the security specialist's responsibilities under the PSP.

Lesson Objectives

- Identify roles and responsibilities of a security specialist
- Determine security reporting requirements
- Explain required security briefings

Security Specialist Duties

Security specialists assist supervisors in determining requirements for individuals requiring access to classified information or for individuals assigned to sensitive positions. They also prepare and request background investigations, evaluate information for temporary (or Interim) national security eligibility, and administer the continuous evaluation program. Security specialists train personnel on the requirements for the Personnel Security Program and conduct briefings for personnel on the necessity of protecting classified information.

To perform all necessary duties, security specialists are required to coordinate with many other offices. You may see a security specialist working with the agency's personnel office, the medical office, the legal office, supervisors, employee assistance programs, and the CAF.

Importance of Reporting

All individuals who have access to classified information or hold a sensitive position must follow strict reporting requirements. They are listed in the SEAD 3 Directive.

These requirements include being required to recognize and avoid personal behaviors and activities that may adversely affect their continued national security eligibility.
Individuals are required to report any activities that might threaten national security and comply with reporting requirements. Failure to do so may result in loss of one's national security eligibility.

Reportable Activities

To ensure the protection of classified information or other information specifically prohibited by law from disclosure, individuals who have national security eligibility shall alert agency heads or designees to the following reportable activities that may be of potential security or counterintelligence (CI) concern.

These activities include, but are not limited to foreign travel, foreign contacts, unwillingness to comply with regulations, unexplained affluence, alcohol abuse, illegal drug use, mental health issues, criminal conduct, violations of national security, and misuse of government property.

Reportable Activities – Noncritical-Sensitive Positions

Reportable foreign activities and other reportable activities for persons with Secret, Confidential, or DOE "L" access and persons assigned to positions designated noncritical-sensitive are listed here.

Secret, Confidential, DOE “L” access, or noncritical-sensitive position reportable activities include:

Foreign Activities:
- Application for and receipt of foreign citizenship
- Application for, possession, or use of a foreign passport or identity card for travel

Other Reportable Activities include:
- Alcohol and drug-related treatment
- Arrests
- Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure, regardless of means
- Media contacts other than for official purposes, where the media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure

Reportable Activities – Critical-Sensitive and Special-Sensitive Positions

Reportable foreign activities for persons with Top Secret, Secret, or DOE "Q" access and persons assigned to positions designated critical-sensitive or special-sensitive are listed here.

Top Secret, DOE “Q” access, critical-sensitive, or special-sensitive position reportable activities include:

Foreign Activities:
- Direct involvement in foreign business
- Foreign bank accounts
- Ownership of foreign property
- Application for, and receipt of, foreign citizenship
- Application for, possession, or use of a foreign passport or identify card for travel
- Voting in a foreign election
- Adoption of non-U.S. citizen children

Other Reportable Activities include:
- Cohabitants
- Marriage
- Financial Anomalies: Including, but not limited to, bankruptcy, garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater

such as an inheritance, winnings or similar financial gain
- Foreign National Roommate(s): Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days

Reportable Activities – Security Specialist Responsibilities

As a Security Specialist you will monitor the effectiveness of reporting requirements and develop recommendations for new or modified requirements, oversee agency compliance, and ensure best practices by identifying, sharing, and implementing them.

Continuous Evaluation Reporting

All individuals who require eligibility for access to classified information or eligibility to hold sensitive positions are responsible for complying with the Continuous Evaluation process. They are made aware of their reporting obligations at initial and annual security awareness training.

They must report changes or incidents that may impact their national security eligibility. If they conceal relevant information during the investigation or after the eligibility was issued, their access can be withdrawn.

Failure to comply with the reporting requirements and resultant determinations may result in administrative action that includes, but is not limited to, revocation of national security eligibility.

Briefing Types

One important responsibility of the security office is to conduct briefings. Security briefings take place to provide important security information to individuals who perform work in a secure environment.

Security specialists take part in four different types of briefings: Initial, annual, insider threat, and termination. Personnel assigned to sensitive duties receive security briefings on the national security implications of their duties and their individual responsibilities.

These briefings will emphasize the individuals' responsibility to meet the standards and criteria for security eligibility as stated in SEAD 4.

Briefing Types - Initial

All personnel with national security eligibility will be given an initial security briefing before being granted access to classified information.

Briefing topics include threat awareness; counterintelligence awareness; an overview of the security classification system; the individual's reporting obligations and requirements; initial cybersecurity awareness; and security procedures and duties applicable to an individual's job.

Briefing Types - Annual

The annual or refresher briefing reminds individuals of their responsibilities under the Personnel Security Program and informs people of any changes in the Personnel Security Program since their last briefing. If a person has a national security eligibility but does not work with classified information on a regular basis, he or she may forget security requirements for the protection of that information. Even if a person frequently works with classified material, he or she may forget some of these requirements. Refresher briefings reinforce good security practices and remind people of the continued need to follow the rules.

Briefing Types – Insider Threats

The purpose of the insider threat briefing is to stress the importance of detecting potential insider threat and make individuals aware of insider threat indicators and reporting requirements. The insider threat briefing includes information on methods used by adversaries to recruit trusted insiders, behaviors that may indicate an insider threat, and insider threat counterintelligence and security reporting requirements.

Briefing Types – Termination

When someone is leaving the military or civilian service with the Federal Government, they are required to receive a termination briefing. This briefing is also required for individuals who have been terminated from employment, have an administrative withdrawal of their access, or will be absent from duty for 60 days or more. Anyone who has inadvertently gained access to classified or sensitive information for which they are not authorized to have access also receives this briefing.

The termination briefing is intended to inform personnel on how to protect classified information, how intelligence services may target personnel after they have left federal service, the legal requirements to protect classified information and criminal penalties for unauthorized disclosure of information, how to report problems, and the need for written approval from the agency before any disclosure. Even when an individual leaves employment, the person still has a legal obligation to protect sensitive and classified information.

Knowledge Check

Question 1 of 3
Which of the following are Security Specialist duties?

- Set date to conduct an annual briefing
- Evaluate Mr. Jones' interim eligibility paperwork
- Call the medical office to inquire about Ms. May's medical records
- Provide applicants with written explanation for negative determination
- Determine whether applicants are reliable enough to access classified information
- Request a national security background investigation for new employee
- Call Mr. Carpenter and assist him with his e-QIP

Question 2 of 3
Which briefing informs personnel on how to protect classified information, how intelligence services may target personnel after they have left federal service, the legal requirements to protect classified information and criminal penalties for unauthorized disclosure of information, how to report problems, and the need for written approval from the agency before any disclosure.

- Initial briefing
- Annual briefing
- Insider threat briefing
- Termination briefing

Question 3 of 3

Individuals with national security eligibility must report which of the following situations?

- Alcohol abuse
- Illegal use or misuse of drugs
- Criminal conduct
- The use of U.S. Government property or information systems

Answers

Question 1 of 3
Which of the following are Security Specialist duties?

- **Set date to conduct an annual briefing**
- **Evaluate Mr. Jones' interim eligibility paperwork**
- Call the medical office to inquire about Ms. May's medical records
- Provide applicants with written explanation for negative determination
- Determine whether applicants are reliable enough to access classified information
- **Request a national security background investigation for new employee**
- **Call Mr. Carpenter and assist him with his e-QIP**

Question 2 of 3
Which briefing informs personnel on how to protect classified information, how intelligence services may target personnel after they have left federal service, the legal requirements to protect classified information and criminal penalties for unauthorized disclosure of information, how to report problems, and the need for written approval from the agency before any disclosure.

- Initial briefing
- Annual briefing
- Insider threat briefing
- **Termination briefing**

Question 3 of 3
Individuals with national security eligibility must report which of the following situations?

- **Alcohol abuse**
- **Illegal use or misuse of drugs**
- **Criminal conduct**
- The use of U.S. Government property or information systems

The Security Specialist Summary

This lesson covered the roles and responsibilities of the security specialist, security reporting requirements for the security specialist, and required security briefings.

Lesson 8: Course Conclusion

Course Summary

The Personnel Security Program aims to protect national security by ensuring that only loyal, trustworthy, and reliable individuals may access classified information or perform sensitive duties. This course has provided you tools and information to understand how personnel security helps protect our nation.

You should now be able to perform the listed activities:

- Demonstrate comprehension of the Personnel Security Program (PSP)
- Explain national security sensitive position designations and special access requirements
- Apply investigative process and comprehend the national security adjudication requirements
- Identify the security specialist's responsibilities under the PSP
- Analyze the continuous evaluation and reinvestigation requirements