Introduction to Personnel Security

Student Guide

August 2017

Center for Development of Security Excellence

Lesson 1: Personnel Security Policy

Lesson Introduction

Overview

Welcome to the Personnel Security Policy lesson. Knowing the history of the personnel security program is an ideal place to start. We only have one section in this lesson, but it's very important in giving you an understanding of where the personnel security program came from, and how it's grown through the years.

At the end of this lesson, you will be able to identify:

- The purpose of personnel security
- The history of personnel security
- Policy documents

Personnel Security Policy

Purpose of Personnel Security

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. The personnel security program establishes the standards, criteria, and guidelines upon which personnel security determinations are based. The personnel security program uses a comprehensive background investigative process in making this determination. It applies to members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated people who require access to classified information, or are assigned to sensitive duties. The goal of the program is to ensure the protection of national security.

What is the National Security?

National security, by definition, encompasses both the national defense and the foreign relations of the U.S. Every nation must be able to defend itself, to ensure its own survival and the survival of its way of life. This ability of our nation to defend itself is one aspect of national security. Another way a nation can defend itself is to maintain a good working relationship with other countries, thereby reducing the threat to our nation's survival. For this reason, foreign relations are also part of how we define national security.

Classified Information

The unauthorized disclosure of 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., information is classified at three levels: Top Secret, Secret, and Confidential. The level of classification of information is determined by the degree of damage to national security that could result from its unauthorized disclosure. Top Secret is the highest level of classification. It is applied to information that reasonably could be expected to cause exceptionally grave damage to the national security if unauthorized disclosure occurs. Secret classification is applied to information that could be expected to cause serious damage to the national security if unauthorized disclosure occurs. Confidential classification is applied to information that reasonably could be expected to cause damage to the national security if unauthorized disclosure occurs. The personnel security program aims to protect national security by determining whether personnel with an official need for access to national security information can be trusted with that information.

Character Traits of Cleared Employees

The United States Government expects cleared employees to be loyal, trustworthy, and reliable. Three questions are asked of everyone who has a need for access to classified information: First, is the individual’s allegiance solely with the United States and its basic form of Government? Second, can the individual be trusted to properly protect classified information and/or perform other sensitive duties? And third, is the individual consistently willing and able to carry out security responsibilities? Since you are here doing this training, the answers to all of the above questions should be “yes.”

Personnel Security Policy

In this section, we will review the history of the personnel security program in order to understand how and why it evolved. Prior to the Civil War, the crimes of spying, lurking behind friendly lines, and giving aid and comfort to the enemy were dealt with severely.

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 political party and the party boss, as opposed to the larger sense of allegiance to the Constitution. It also carried with it a presumption of allegiance. The employee was presumed to be loyal because in the past, he had been 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 was a powerful impetus for remaining loyal.

Because of the many abuses of the spoils system, such as incompetent and corrupt public officials, or civil servants who felt they were working for the party rather than the American people, the Civil Service Act was passed in 1883. The Civil Service Act created the U.S. Civil Service Commission. The act required that employees be appointed on the basis of ability, which was demonstrated by taking an exam. This created a concern about the loyalty

of federal employees, since they were no longer dependent upon the party favor to keep their jobs. Their allegiance could no longer be "bought" or necessarily even depended upon.

Eventually, Congress passed the Hatch Act in 1939 to address this problem. The Hatch Act represents the beginning of the present-day personnel security program. According to this act, federal employees must be loyal to the United States.

History of Personnel Security Timeline

Year	Event
1939	**The Hatch Act** This act represents the beginning of the present-day Personnel Security Program within the United States. The Hatch Act ordered the immediate removal of any person advocating the overthrow of the United States by unlawful means.
1941	During the 1940s, questions were added to federal employment applications which asked about membership is subversive organizations and specifically mentioned Communist and German Bund organizations. In 1941, President Roosevelt issued **Executive Order 8781** which required fingerprinting of every employee whose prints were not already on record. In addition, President Roosevelt directed the Federal Bureau of Investigation to establish a system to check criminal records.
1942	The **War Service Regulation II**, issued in February 1942, denied examination or appointment to anyone whose loyalty was in reasonable doubt and denied appointment to those actively associated with Nazi, Fascist, and Japanese groups, or were members of the Communist Party.
1947	After World War II, President Truman issued **Executive Order 9835**, which implemented recommendations resulting from extensive congressional study. The order established the standard that federal employment will be refused if the evidence shows that “reasonable grounds exist for the belief that the person involved is disloyal to the Government of the United States of America.”
1953	**Executive Order 10450** All persons privileged to be employed in the departments and agencies of the government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. —Issued by President Eisenhower, April 27, 1953
1987	**DoD Regulation 5200.2-R, January 1987** This regulation established the DoD personnel security program and the various requirements that supported the program. It has since been replaced by the DoD Manual 5200.02.

Year	Event
1995	**E.O. 12968, Access to Classified Information**, establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information (August 2, 1995).
2004	**The Intelligence Reform and Terrorism Prevention Act (2004)** Title III streamlines the investigative and adjudicative processes. In 2004 the Intelligence Reform and Terrorism Prevention Act (IRPTA) was enacted to reform the intelligence and intelligence-related activities of the United States Government among its other purposes.
2005	**Adjudicative Guidelines** Implementation of Adjudicative Guidelines for Determining Eligibility For Access to Classified Information (December 29, 2005) replaced the guidelines published in DoD 5200.2-R and DoD Directive 5220.6. However, the 2005 guidelines have been replaced by new National Security Adjudicative Guidelines effective June 8, 2017

Policy Documents/Executive Orders

There is a long and rich history that has brought us to the personnel security program that we have today. This program has been built one block at a time. Through time and experience, our government has learned just what it takes to protect our national security. The personnel security program is governed by several executive orders and policies.

- **Executive Order 10450** (27 Apr 53) manages federal civilian employees.
- **Executive Order 10865** (20 Feb 60) manages federal contractors under the Industrial Security Program, with some modifications under E.O. 12829.
- **Executive Order 12968** (2 Aug 95) establishes the personnel security program for the executive branch of the federal government. It also regulates access to classified information.
- **Executive Order 13467** (30 Jun 08) designates the Director of National Intelligence as the "Security Executive Agent" 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. It also creates the suitability and Security Clearance Performance Accountability Council, and further authorizes continuous evaluation of personnel who hold active security clearances.

These Executive Orders are available on the Course Resources page.

Policy Documents/Regulations and Guidelines

The 2014 DoD Instruction 5200.02 establishes policies, assigns responsibilities, and prescribes procedures for the DoD Personnel Security Program. The DoD personnel security program and its major elements are mandated and regulated by the 2017 DoD Manual 5200.02, Procedures for the DoD Personnel Security Program, which serves as the mandatory document for use by all DoD components.

In addition to DoD Instruction 5200.02, and the DoD Manual 5200.02, there have been several regulatory changes consistent with Executive Order 12968.

Passed in 2008 the Bond Amendment repealed Title 10 U.S.C. Section 996 formerly known as the Smith Amendment, and places restrictions that are similar to the Smith Amendment, but which apply to all Federal Government Agencies. The Bond Amendment bars persons from holding a security clearance for access to SAPs, Restricted Data and SCI if they have been: convicted of a crime and served more than one year of incarceration; discharged from the Armed Forces under dishonorable conditions or were determined to be mentally incompetent by a court or administrative agency. The Bond amendment also prohibits all Federal Agencies from granting or renewing a security clearance for any covered person who is an unlawful user of a controlled substance or is an addict; this prohibition applies to all clearances.

And the Director of National Intelligence, or DNI, signed revised National Security Adjudicative Guidelines in December 2016, outlined in the Security Executive Agent Directive, or SEAD, 4. These adjudicative guidelines were effective 180 days after the DNI's signature. Any executive branch agency authorized or designated to conduct adjudications to determine eligibility for initial or continued access to classified national security information or eligibility to hold a sensitive position was required to implement the new national security adjudicative guidelines by June 8, 2017. These new adjudicative guidelines replace the December 2005 guidelines.

Summary

By this point you should understand how personnel security has evolved and why it is so important. To review, the personnel security program seeks to ensure that only loyal, trustworthy, and reliable people are granted access to classified information or assigned to 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.

There are several documents that mandate the personnel security program.

- DoD Instruction 5200.02 (March 2014) establishes the policy, assigns responsibilities, and prescribes procedures for the DoD Personnel Security Program.

- DoD Manual 5200.02 implements policy for the major elements of the personnel security program.
- Executive Order 12968 was the most recent executive order that required several regulatory changes to the DoD Personnel Security Program. As a security professional you will become familiar with these documents.

Review Activity: Personnel Security Policy

Match each term or phrase to its description. Check your answer in the Answer Key at the end of this Student Guide.

Terms:

A. Spoils System

B. E.O. 10450

C. DoDI 5200.02

D. Loyal, trustworthy, reliable

E. Civil Service Commission

F. Hatch Act, 1939

Descriptions:

_____ Character traits looked for in a government employee

_____ System that required allegiance to a political party and not the Constitution

_____ The Civil Service Act of 1883 created this

_____ Act that represents the beginning of the Personnel Security Program

_____ The Executive Order that managed federal civilian employees

_____ DoD instruction that establishes the policy, assigns responsibilities, and prescribes procedures for the DoD Personnel Security Program

Lesson 2: DoD Personnel Security Program

DoD Personnel Security Program

Overview

Welcome to the DoD Personnel Security Program lesson. At the end of this topic, you will be able to describe the authority for this Department of Defense program, as well as the five elements of the personnel security program.

Authority

The personnel security program is governed by several executive orders that cover different facets of the program.

Security considerations for civilian employees of the federal government are governed by executive order 10450.

With some modifications under E.O. 12829, executive order 10865 governs contractors under the industrial security program.

Executive Order 12968 grants authority for the standardized procedures that govern DoD personnel security policy. This executive order establishes a uniform Federal Personnel Security Program for employees who will be considered for initial or continued access to classified information. This executive order also sets forth the standard for access eligibility to include: adjudicative policy, investigative standards, and reciprocal acceptance of access eligibility determinations within the Executive Branch.

Executive Order 13467 appoints the Director of the Office of Personnel Management as the Suitability Executive Agent and Director of National Intelligence as the Security Executive Agent.

In addition to these executive orders, DoD Manual 5200.02 establishes the personnel security program for the DoD.

Finally, the Intelligence Community Directive 704 (ICD 704) establishes the policy that governs eligibility for access to Sensitive Compartmented Information (SCI).

Elements of the Personnel Security Program

There are five elements to the Personnel Security Program. These elements are an integral part of the program.

Designation

Each position in the Federal service is evaluated for a position designation. The designation is based on how the responsibilities and assignments of the position could impact the national security.

Positions designated as sensitive involve job duties that can have a great impact on national security, as the individual assigned to the position could bring about, by virtue of the nature of the position, a material adverse effect on the national security.

Positions with job duties which have no potential for material adverse effect on national security are designated as non-sensitive. If a position is designated as having sensitive duties, the remaining four elements will apply.

Investigation

Once an individual has been selected for a sensitive position and/or requires access to classified information (military, civilian, or contractor) a personnel security investigation (PSI) is conducted. The PSI report contains background information about the person.

Adjudication

This is an evaluation of the information contained in reports of personnel security investigations (PSIs) and other source documents.

A judgment concerning security clearance eligibility is made by evaluating the reported information against the national security adjudication adjudicative guidelines. Final clearance eligibility determinations decisions are made by the DoD Consolidated Adjudications Facility (CAF).

Reinvestigation

Individuals are reinvestigated at certain intervals based on their duties or access.

Reinvestigation may also be initiated when unfavorable information arises that raises a concern under the national security adjudicative guidelines. Reinvestigation is considered part of the Continuous Evaluation Program.

Continuous Evaluation

Once security clearance eligibility has been granted, the Continuous Evaluation Program (CEP) monitors employees for new information or changes since the last investigation or reinvestigation that could affect their eligibility status.

Summary

The information you learned in the last two topics begins to lay a foundation for what is ahead as you learn more about the Personnel Security Program.

Although the personnel security program is governed by several executive orders, Executive Order 12968 is the most prominent. It standardized procedures for DoD personnel security policy.

The five elements of the personnel security program that we covered are:

- Designation
- Investigation
- Adjudication
- Reinvestigation
- Continuous evaluation

Review Activity: DoD Personnel Security Program

Match each term to its description. Check your answer in the Answer Key at the end of this Student Guide.

Terms:

A. Continuous Evaluation

B. Reinvestigation

C. Adjudication

D. Investigation

E. Designation

Descriptions:

_____ An assessment of a position's potential impact on the national security is a part of this process.

_____ A judgment concerning security clearance eligibility is made by evaluating the information in the PSI with DoD standards.

_____ This is part of the CEP. It is done at certain intervals based on duties or access.

_____ A report is generated from this that contains information about an individual who has been selected for special duties. The report is used to evaluate the individual for eligibility.

_____ This is used to monitor employees for new information or changes that could affect their status.

Sensitive Duties

Overview

As a security professional, you will often hear people talk about sensitive duties or positions, and you may need to process individuals for access to classified information or assignment to a sensitive position. At the end of this topic, you will be able to explain:

- Access to sensitive duties
- Requirements of sensitive duties
- Civilian personnel designations

Access

Sensitive duties are designated based on their impact on national security. Sensitive duties often involve access to classified information.

Access is described as the ability and opportunity to gain knowledge of classified information. This can involve seeing, hearing, or touching classified information, material, or equipment. Access is always controlled by the holder of the information. The holder of the classified information must determine that the person seeking access has the proper security clearance eligibility and a valid need to know the information in order to carry out official duties.

A security clearance eligibility is a favorable determination for access to classified information or assignment to a sensitive position prior to access being granted. Component and local command procedures will provide guidance on how to verify clearance eligibility and need-to-know.

Requirements

Not just anyone can access classified information. There are two basic types of authorizations for granting access. First, if an individual is a U.S. citizen, he or she may be granted a security clearance eligibility. Next, non-U.S. citizens, in rare instances, may be granted 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 be granted an LAA, they are not granted security clearance eligibility.

Personnel Designations

Civilian personnel designation requirements vary based on how the position is categorized. They can be categorized in one of four ways:

- Special-sensitive

- Critical-sensitive
- Noncritical-sensitive
- Non-sensitive

Where there is a mix of duties, the highest level of duty determines the sensitivity. The designation of sensitive positions meet the stated criteria for a specific security designation and are necessary to meet mission requirements. In addition, some civilian positions do not require access to classified information but involve performing duties which impact the national security, and as result are designated as sensitive positions. Military and contractor personnel have designations distinct from civilian employees. Both may have access to classified information and have sensitive duties comparable to civilians.

Last, but by no means any less important, is the Limited Access Authorization, also known as LAA. An LAA may be granted when it is in the interest of the U.S. Government to allow a non-U.S. citizen to have access to classified information. An example of this would be assigning duties to a non-U.S. citizen with special expertise or knowledge that is not available from a U.S. citizen in that position.

Special-Sensitive

Special-Sensitive and Critical-Sensitive duties are the most sensitive duties within DoD.

Special-Sensitive position: A civilian national security position with potential for inestimable damage to the national security or inestimable adverse impact to the efficiency of the DoD or Military Services:

- Positions requiring eligibility for access to Sensitive Compartmented Information (SCI)
- Positions that require access to unique or uniquely productive intelligence-related special sensitive information or involvement with Special Access Programs (SAPs)
- Any civilian position the DoD Component head determines to be at higher level than critical-sensitive due to special requirements

Critical-Sensitive

Special-Sensitive and Critical-Sensitive duties are the most sensitive duties within DoD.

Critical-Sensitive positions: A civilian national security position that has the potential to cause exceptionally grave damage to the nation’s security, including but not limited to:

- Top Secret duties

- Eligibility for access to Top Secret or Department of Energy (DOE) “Q” level classified information
- Development or approval of war plans, war operations, or critical and extremely important items of war
- National security policy making or determining duties having potential to cause exceptionally grave damage
- Investigative duties involving counterintelligence (CI) or background investigations that have the potential to cause exceptionally grave damage to the national security
- Duties related to adjudication, adjudicative determination recommendations, or granting of national security eligibility
- Duties on personnel security boards
- Duties involving development or approval of plans, policies, or programs that impact DoD operations
- Duties involving the conduct of CI activities
- Senior management positions in key programs that could result in grave damage if compromised
- Positions having direct involvement with diplomatic relations/negotiations
- Positions involving independent responsibility for planning or approving continuity of government operations
- Positions in which the occupant has the ability to independently damage public health and safety with devastating results
- Positions in which the occupant has the ability to independently compromise or exploit biological select agents or toxins, chemical agents, nuclear materials, or other hazardous materials
- Positions in which the occupant has the ability to independently compromise or exploit the nation’s nuclear or chemical weapons designs or systems
- Positions in which the occupant has direct, unrestricted control over supplies of arms, ammunition, or explosives or control over any weapons of mass destruction
- Positions in which the occupant has unlimited access to and control over classified information, but only where the unauthorized disclosure of that information could 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, or procurement or securing funding for goods or services with monetary value in excess of $50 million annually
- Positions designated by the DoD Component head

Noncritical-Sensitive

Noncritical-Sensitive duties are sensitive and can damage national security, though not as severely as critical duties.

Noncritical-Sensitive positions: A civilian national security position with the potential to cause significant or serious damage to the national security

- 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 or information pertaining to Service members that is otherwise protected from disclosure, which has the potential to cause serious damage to the national security
- Positions designated by the DoD Component head

Non-Sensitive

All remaining civilian employee positions are designated as Non-sensitive. This means that there are no sensitive job duties and/or need for access to classified information, and that the position does not have the potential to adversely impact the national security.

Mixed-Civilian Designations

Where there is a mix of duties, the highest level of duty determines the sensitivity.

Mixed-civilian designations:

- Required when a sensitive position involves a mix of Critical-Sensitive and Noncritical-Sensitive duties

Examples of duties with mixed-civilian designations:

- Base Comptroller

- Duties include obligating over $200 million in funds per year
- Requires eligibility for access to secret information
- The fiduciary responsibilities designate the position critical–sensitive, even though the access level requirement is only secret

Military/Contractor Designations

Military and contractor personnel have designations distinct from civilian employees.

Both military and contractor personnel have:

- Access to classified information
- Perform sensitive duties comparable to civilians

Limited Access Authorization (LAA)

When non-U.S. citizens require classified access to perform official duties, they can be granted a Limited Access Authorization (LAA). The LAA is used when it is not possible or not practical to use U.S. citizens for certain duties, and in the interest of the U.S. Government to allow the non-U.S. citizen to have access. A non-U.S. citizen may be granted an LAA, but they are not granted security clearance eligibility. Note: The investigative requirement for an LAA is a Tier 5.

An LAA can be granted to civilian, military, or contractor personnel.

With LAA access:

- Access is limited to the approved program or project
- Access outside of the approved program or project is a compromise and must be handled as one
- Information must be releasable to the applicant's home country under the U.S. National Disclosure Policy
- Access is limited to Secret information or lower

Positions Not Requiring Access to Classified Information

Some duties may give untrustworthy individuals an opportunity to endanger national security, even without granting access to classified information. A command may therefore require a security investigation for individuals assigned to these duties.

Examples of Positions Not Requiring Access to Classified Information:

- Red Cross and/or United Service Organizations personnel
- Non-U.S. citizens employed by DoD components overseas

- Personnel occupying some IT or related positions

The positions may apply to civilian, military, and contractor personnel. The non-U.S. citizen status of the person holding such a position or performing such duties is not an automatic disqualifier.

Summary

In this section, you learned who can obtain access to classified information and what the requirements are to make that happen.

Designations and requirements are based on the sensitivity of the duties that need to be performed. Recall that there are several different factors that determine how designations are made.

Review Activity: Sensitive Duties

Read the scenario below and then select the best response to the questions that follow. Check your answer in the Answer Key at the end of this Student Guide.

Joe Smith is a Division Chief who works in a Federal Government agency where he has several individuals working for him. With civilians, contractors, and military personnel in his office, he sometimes finds it difficult to keep the designations for all of his people straight.

Question 1 of 6. The majority of Joe's employees are civilians who work on very sensitive projects that require access to Top Secret information. These civilian employee positions are categorized as which of the following?

- ○ Non-Critical Sensitive
- ○ Critical Sensitive
- ○ Special Sensitive

Question 2 of 6. Two civilians who require access to Sensitive Compartmented Information have position sensitivity categories of which of the following?

- ○ Non-Critical Sensitive
- ○ Critical Sensitive
- ○ Special Sensitive

Question 3 of 6. Most military personnel who work in the office must have *(fill in the blank)* to classified information at the Top Secret or Secret level in the official performance of their duties.

- ○ Access
- ○ Limited Access Authorization

Question 4 of 6. The Comptroller of the base also reports to Joe. This person's civilian position is categorized as Critical Sensitive due to fiduciary duties requiring procurement of services in excess of *(fill in the blank)*.

- ○ $500,000
- ○ $500 million
- ○ $50 million

Question 5 of 6. He also has a few employees who develop and deliver instruction to other DoD employees at the agency. Their duties are sensitive and could potentially damage national security if information was leaked; however, the information would not be as harmful as that from a Critical Sensitive designation. Which designator do these individuals have?

- ○ Public Trust
- ○ Non-Critical Sensitive
- ○ Special Sensitive

Question 6 of 6. Joe also has an individual on temporary assignment working in his office. He is a member of the Royal Navy, and as such is a British citizen. In the position he is filling, it is not possible or not practical to use a U.S. citizen. For this reason, he has been granted which of the following?

- ○ Access
- ○ Clearance
- ○ Limited Access Authorization

Joe is very security conscious therefore, he tries to make sure that each of his employees understands the limits of the designations that their jobs have been given.

Special Access Requirements

Overview

The next section will briefly introduce special requirements for access to information related to programs that impose access controls beyond those normally provided to Confidential, Secret, or Top Secret information. At the end of this topic, you will be familiar with:

- Special Programs
- Restricted Data and Critical Nuclear Weapon Design Information (CNWDI)

Special Access Programs

Several programs, known as Special Programs, provide an additional layer of security to some of our nation's most sensitive assets. These programs cover a variety of areas, including:

- Presidential Support Activities
- Special Access Programs
- NATO
- Nuclear Personnel Reliability Program (Nuclear PRP)
- Sensitive Compartmented Information (SCI)
- Nuclear Command and Control – Extremely Sensitive Information (NC2-ESI)
- Chemical PRP

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

Nuclear Personnel Reliability Program (Nuclear PRP)

The Nuclear Personnel Reliability Program (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 has demonstrated reliability and professional competence.

Restricted Data and CNWDI

In addition to the specific categories of information covered by Special Access Programs, Restricted Data and Critical Nuclear Weapon Design Information, or CNWDI, also have special requirements for access and dissemination. Restricted Data includes all information concerning the design, manufacture, or use of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy. Note that

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. Critical Nuclear Weapon Design Information is Restricted Data that is classified as Top Secret or Secret. It includes information about the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition, or test device.

Requirements for access to this type of information will be covered in Lesson 3.

Summary

As a security professional, you will certainly learn more about these special programs in the future. For now, keep in mind that it is imperative that the information in these programs be protected from anyone who does not have a need-to-know.

Special Programs (SAPs):

- Presidential Support Activities
- NATO
- Nuclear Personnel Reliability Program (Nuclear PRP)
- Sensitive Compartmented Information (SCI)
- Nuclear Command and Control – Extremely Sensitive Information (NC2-ESI)
- Chemical PRP

Other Special Access Issues:

- Restricted Data
- Critical Nuclear Weapon Design Information (CNWDI)

Review Activity: Special Access Requirements

For each statement, select True or False. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 2. Special access requirements are designed to provide an additional layer of security to some of our nation's most valuable assets.

- ○ True
- ○ False

Question 2 of 2. Having an active security clearance eligibility makes one eligible to access all classified information.

- ○ True
- ○ False

Security Office

Overview

The security office plays an important role in the personnel security program. This topic covers the duties performed within the security office, the briefings security professionals conduct, and the role they play with regards to the electronic questionnaire (e-QIP system) during the investigation process.

Duties

As a security professional, it is important that you have a clear understanding of what the security officer duties are. They include:

- Assisting supervisors in determining sensitivity for both access and assignment to sensitive duties
- Preparing and requesting personnel security investigations
- Evaluating information for interim security clearances
- Administering the continuous evaluation program
- Training personnel on the requirements for the personnel security program
- Conducting briefings for personnel on the necessity of protecting classified information

To perform all of their duties, the security officer has to coordinate with many other offices. You may see the security officer working with:

- The personnel office
- The medical office
- The legal office
- Supervisors
- Employee assistance programs
- The DOD Consolidated Adjudications Facility (CAF)

Now that you know all of the people and offices that the security officer has to coordinate with, you can see what an important role they play in the personnel security mission.

Briefings

One important responsibility of the security office is to conduct briefings. A briefing is defined as the act or instance of giving instructions or preparatory information to someone. Security briefings are conducted to provide important security information to individuals who perform

work in a secure environment. As a security professional, you will be exposed to four different types of briefings:

- Initial briefing
- Annual or refresher briefing
- Insider Threat briefing
- Termination briefing

Security briefings are an important source of information, and play a key part in the personnel security program.

The Initial Briefing

The initial briefing is given to personnel who have recently been approved and granted access to classified information. This briefing includes such information as the importance of classified information, the proper ways to protect classified information, how to perform the duties that require access, and potential security concerns with foreign intelligence services. Procedures to report any issue associated with the protection of classified information are also addressed.

The Annual Briefing

The annual or refresher briefing is used to remind people about their responsibilities under the personnel security program, and to inform people of any changes in the personnel security program since their last briefing. If a person has a clearance 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. The refresher briefing is intended to reinforce good security practices, and remind people of the continuing need to follow the rules.

The Insider Threat Briefing

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 which may indicate an insider threat, and insider threat counterintelligence and security reporting requirements.

The Termination Briefing

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. This type of

briefing is also given to anyone who has inadvertently gained access to classified or sensitive information for which they are not authorized to have access.

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 is no longer employed, he or she still has a legal obligation to protect sensitive and classified information.

Role in e-QIP

Among its many other responsibilities, the security office plays a key role in the process of applying for personnel clearances using the "e-QIP", or Electronic Questionnaires for Investigations Processing, system. First, using e-QIP, the security office initiates a personnel security questionnaire. Next, the individual being investigated must complete the e-QIP electronic questionnaire and the security office may assist with this process. Once the individual has completed the questionnaire, the security office reviews and approves the questionnaire, and then forwards the electronic questionnaire to the National Background Investigations Bureau, or NBIB, a newly formed semi-independent entity within the Office of Personnel Management (OPM) to begin the next step in the investigative clearance process. If the security office should need to track the status of the investigation and clearance process, they can do so through the current DoD System of Record.

As a security professional, you will no doubt be involved in this process at some point in your career.

Summary

The security office has many responsibilities and you will learn about them in more detail in the near future. Security officers may find themselves assisting supervisors in determining sensitivity for access, initiating personnel investigations, evaluating interim eligibility information, operating the continuous evaluation program, and conducting briefings.

Review Activity: Security Office

Which of the following are security office duties?

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

- ☐ set date to conduct an annual briefing
- ☐ evaluate Mr. Jones's interim eligibility paperwork
- ☐ call the medical office about Ms. May
- ☐ request personnel security investigation for new employee
- ☐ call Mr. Carpenter and assist him with his e-QIP
- ☐ plan the holiday party for the security office
- ☐ order cleaning supplies
- ☐ set a date to conduct training on personnel security requirements

Lesson 3: Security Clearance Eligibility Process

Security Clearance Eligibility Process

Overview

Welcome to the Security Clearance Eligibility Process lesson. Over the next couple of sections, we are going to discuss what a security eligibility is, how it is processed, and how it is granted. You will also learn about restrictions and what access means. As a security professional this knowledge will be very valuable to you.

What is a Security Clearance?

What exactly is a security clearance eligibility? A security clearance eligibility is a favorable determination that an individual is eligible for access to classified information or assignment to sensitive duties at specific levels prior to access being granted. Although a security clearance eligibility is a favorable determination of eligibility for access to classified information, it does not guarantee access to that information. The ultimate authority for granting access to classified information rests with the local command or activity.

Granting a Security Clearance

To establish the need for a security clearance eligibility, an assessment of an individual's specific situation and or position must be completed to define regular access. The Department of Defense does not define regular access in terms of specific time periods. Regular access could be defined as daily, weekly, or even monthly depending on the need. Once an individual's need for regular access has been confirmed, there is a standard process that must be followed in order to grant a security clearance eligibility.

Clearance Process

The process for granting a security clearance eligibility is certainly something that you will become familiar with as a security professional. For the most part, the granting of a security clearance eligibility is done in four phases. The first phase is when a personnel security investigation (PSI) is initiated and completed on an individual. Once the PSI is completed, it is forwarded to the Department of Defense Consolidated Adjudications Facility (DoD CAF). This is the second phase. The third phase is when the DoD CAF reviews the information in the PSI and compares it to national adjudication standards. The final phase is when the DoD CAF makes a determination and either grants a security clearance eligibility or not.

Restrictions

Not just anyone can obtain a security clearance eligibility. Let's say, for instance, an individual receives an unfavorable adjudication determination after due process. This means

that the individual will be restricted from obtaining a security clearance eligibility. In addition, there are a few other individuals who are restricted from receiving clearance eligibility. They include non-U.S. citizens, civilians in non-sensitive 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." The individuals just described are not in a position where they "need to know" and, therefore, do not need access.

Access

Having a security clearance eligibility does not give one carte blanche access. As a security professional, you will often hear and use the term "need-to-know." Before an individual can be granted access to any classified information, he or she must have a security clearance eligibility for that level of information, have signed the Non-Disclosure Statement SF-312 and have an official need-to-know. Simply having the eligibility does not constitute a need-to-know. Prior to disclosing classified information, it is the responsibility of the person who holds the information to ensure that the recipient has the appropriate clearance eligibility and the need to know. As a security professional, it is your responsibility to make sure that these access rules are adhered to in the interest of protecting classified information. Note that there are additional requirements for Restricted Data and Critical Nuclear Weapon Design Information (CNWDI).

Restricted Data

Within and between DoD components, access to and dissemination of Restricted Data are governed by the same basic requirements that govern access to and dissemination of other classified information. That is, access is granted only if it is required for performance of official duties and only to individuals who hold a valid DoD security clearance eligibility at a level commensurate with the information. Likewise, information is disseminated only after the holder of the information has verified the identity of the prospective recipient, the validity of the recipient's clearance eligibility, and the recipient's need to know.

Critical Nuclear Weapon Design Information (CNWDI)

Controlling access to and dissemination of CNWDI is particularly important to the DoD. Because of its extremely sensitive nature, access must be limited to the absolute minimum number of people who need it to accomplish their job duties. Like other types of classified information and Restricted Data, access is limited to individuals who have a security clearance eligibility for that level of information and an official need-to-know.

However, the requirements for access to CNWDI are much more stringent than for other types of classified information. First of all, the minimum required security clearance eligibility for access to CNWDI is Top Secret or Secret. Secondly, except in rare instances, U.S. citizenship is required for access to CNWDI. Any exceptions will be granted by the Secretary of Defense or his designee. And lastly, written or oral

communication of CNWDI is strictly limited to personnel with a justified and documented need to know.

Summary

In this section, you have learned that a security clearance eligibility is a favorable determination that an individual is eligible for access to classified information or assignment to sensitive duties. You have also learned what access is and that regular access could be daily, weekly, or even monthly, depending on the job. In addition, you learned the phases of obtaining a security clearance eligibility, which include the personnel security investigation, the adjudication phase, and a determination by the CAF. You should also recall that we discussed certain individuals who are restricted from obtaining a clearance eligibility. Among those individuals are non-U.S Citizens and civilians in non-sensitive positions.

Review Activity: Security Clearance Eligibility Process

For each statement, select whether it is fact or fiction. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 4. Joe Smith received an unfavorable security clearance eligibility determination. He is now able to go and work on the classified project that he has wanted to work on.

- ○ Fact
- ○ Fiction

Question 2 of 4. The Department of Defense does not define regular access in terms of specific time periods. Joe could need access just once a week or even monthly and that could be defined as regular access.

- ○ Fact
- ○ Fiction

Question 3 of 4. The first phase of the security clearance eligibility process is the personnel security investigation.

- ○ Fact
- ○ Fiction

Question 4 of 4. Even though Mr. Curly is a citizen of Germany he will be able to have access to any classified information anywhere once he has obtained his Limited Access Authorization (LAA).

- ○ Fact
- ○ Fiction

Key Concepts

Overview

As a security professional, there are a few key concepts that you will hear quite often. In this section lesson, we are going to cover three of them that will be imperative for you to understand. They are personnel security investigations, need-to-know, the provisions of the Privacy Act of 1974, and reciprocity.

Personnel Security Investigation

A personnel security investigation, also known as a PSI, is an inquiry into an individual's background, activities, and personal behavior for the purpose of making a personnel security determination. A PSI allows adjudicators to look closely at important information about an individual's honesty, reliability, character, loyalty, and trustworthiness.

The PSI is used to determine the eligibility of an individual for access to classified information, acceptance or retention into the armed forces, assignment or retention in sensitive duties, or other designated duties requiring investigation. DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with DoD, are all subject to PSIs as the basis for security clearance eligibility determinations.

Need-to-Know

Another term you will see and use often as a security professional is need-to-know. Even when an individual holds a security clearance eligibility, he or she is not automatically given access to all material that is classified. The only access that is authorized is for what the individual has an official need-to-know in order to conduct his or her duties.

Privacy Act

The Privacy Act of 1974 is a public law that regulates the federal government's authority to collect personal information on an individual. This act limits the use of information collected for specific purposes. When the federal government collects personal information from an individual, it is required that the individual be informed of four things:

1. Under what authority is the government agent or representative collecting the information?
2. The purpose for collecting the information.
3. The routine uses of the information.
4. Whether providing this information is voluntary or mandatory, and what would be the impact of choosing not to provide the information?

The Privacy Act Advisement that is found at the end of all investigative forms serves to inform the individual of these provisions.

Reciprocity

Reciprocity refers to the mutual acceptance of a personnel security clearance eligibility by all government agencies, regardless of which agency issued the clearance. A personnel security clearance eligibility should be reciprocally accepted by all federal agencies as long as it meets or exceeds the level of clearance needed by an agency. Furthermore, except in extenuating circumstances, background investigations and eligibility determinations conducted under Executive Order 12968 shall be mutually and reciprocally accepted by all agencies.

According to the NISPOM, each agency that grants its employees access to classified information is responsible for determining whether those employees have previously been cleared or investigated by the federal government. The NISPOM goes on to address the contractor's responsibility to not request a personnel security clearance eligibility to one agency if the employee applicant is already cleared or is in process for clearance eligibility by another agency.

Whether working for the government or for a contractor, a previously cleared individual is not subject to a new investigation or adjudication unless the previous clearance 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.

Summary

Recall that PSI stands for personnel security investigation and that need-to-know policy requires that classified information only be accessible when official duties require it. The Privacy Act requires that each individual asked to provide personal information be advised of the following four points: Authority, Principal Purposes, Routine Uses, and Voluntary or Mandatory Nature of Disclosure. And finally, reciprocity refers to the mutual acceptance of a personnel security clearance eligibility by all government agencies, regardless of which agency issued the clearance.

Review Activity: Key Concepts

When the federal Government collects personal information from an individual, it is required that the individual be informed of which of the following?

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

- ☐ Under what authority the Government agent is collecting the information
- ☐ The purpose for collecting the information
- ☐ The routine uses of the information
- ☐ Whether providing this information is voluntary or mandatory

Clearance Software

Overview

In this section, we are going to discuss the three different electronic systems that are used in personnel security to assist with the process of security clearances. Those three systems are called Electronic Questionnaire for Investigative Processing (e-QIP), Joint Personnel Adjudication System (JPAS), and Case Adjudication Tracking System (CATS).

In the near future, JPAS will be replaced by the Defense Information System for Security, or DISS.

e-QIP

When an individual begins the process of obtaining a security clearance, the security office will initiate the process. The first thing that the subject of the investigation will do after notification from the security office is use the Electronic Questionnaires for Investigations Processing system (e-QIP) to electronically enter all their personal data.

There are many advantages to using e-QIP. The U.S. Government's Office of Personnel Management (OPM) owns and manages the e-QIP system. e-QIP completely automates investigation forms and using this software to fill out the forms reduces the number of errors on applications. e-QIP allows an individual to update the questionnaire by simply making changes on the existing stored e-QIP form, often without having to fill out any additional forms. Perhaps the most significant advantage to using e-QIP is that it reduces delays in investigations, which allows individuals to obtain eligibility, and begin working on classified projects as soon as possible.

The e-QIP program requires several steps to be completed by both the subject of the investigation and the security office. More detailed information on e-QIP will come later in your training.

JPAS

Those individuals working in the personnel security field perform many of their personnel security actions using the Joint Personnel Adjudication System (JPAS). However, it is important to know that in the near future, the Defense Information System for Security (DISS) is a new system that when fully deployed is designed to replace JPAS.

JPAS is the Department of Defense system that uses the Web to connect security personnel around the world with a database managed by the DoD Consolidated Adjudications Facility, (CAF). JPAS uses a centralized database with centralized computer processing and application programs for standardized DoD personnel security processes.

JPAS is comprised of two major sub systems. They are:

- JCAVS, the Joint Clearance and Access Verification System
- JAMS, the Joint Adjudication Management System

JCAVS

JCAVS provides the ability to constantly update accesses and related information in real-time, along with the ability to constantly communicate with other Security Management Offices and CAFs. JCAVS also provides the ability to manage personnel actions, run reports, and receive notifications. JCAVS is used by security professionals throughout the DoD, including contractors.

JAMS

JAMS provides the DoD CAF a single information system to assist in the adjudication process, standardizes core DoD Adjudication processes, and is used by adjudicators to record eligibility determinations and recommend access decisions. JAMS promotes reciprocity between the DoD CAF and the security professional.

CATS

In April 2009, USDI designated CATS as the DoD Case Adjudication Tracking System for all non-intelligence activities. CATS is used by the DoD CAF adjudicators to review electronic PSIs completed by the National Background Investigations Bureau (NBIB). With CATS the adjudicator can record eligibility and can recommend access determinations.

Summary

This section has covered a lot of information at one time, especially for someone who is new to the security field. In the future you will no doubt be exposed to the two electronic systems, e-QIP and JPAS. You will learn much more about them as time goes on and you begin to work with the systems.

Let's review what we have learned. Let's start with e-QIP, OPM's system which is used to automate all investigative questionnaires. It allows a subject of an investigation to enter all their personal data, and know that it is safe due to being on a secure network.

You will also use the JPAS system. JPAS is made up of two major sub-systems that are called JCAVS and JAMS. JCAVS stands for Joint Clearance and Access Verification System, and is used by security professionals throughout the Department of Defense including contractors. JAMS, the Joint Adjudication Management System, is used by the DoD Consolidated Adjudications Facility.

The Case Adjudication Tracking System, CATS, is the DoD Case Adjudication Tracking System for all non-intelligence activities. However, as stated previously, it is important to know that in the near future, the Defense Information System for Security (DISS) is a new

system that when fully deployed is designed to replace JPAS. DISS consists of two main components, the Case Adjudication Tracking System (CATS) and the DISS Portal.

Review Activity: Clearance Software

Select the best response to each question. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 4. What system does Mr. Smith need to access when he needs to update his personal information prior to a reinvestigation?

- ○ e-QIP
- ○ JPAS
- ○ JCAVS
- ○ JAMS

Question 2 of 4. If Mr. Smith's security manager needs to communicate with a CAF he would use what system?

- ○ e-QIP
- ○ JPAS
- ○ JCAVS
- ○ JAMS

Question 3 of 4. JCAVS and what other sub-system make-up the JPAS system?

- ○ e-QIP
- ○ JPAS
- ○ JCAVS
- ○ JAMS

Question 4 of 4. Which system is the Department of Defense system that uses the Web to connect security personnel around the world?

- ○ e-QIP
- ○ JPAS
- ○ JCAVS
- ○ JAMS

Personnel Security Investigations

Overview

This section topic will provide you with a foundation of knowledge about personnel security investigations and will cover the following information:

- The definition of a personnel security investigation
- The purpose of the investigation
- What you need to know about personal information
- The information advisement to the subject of the investigation
- The investigative agency responsible for the personnel security investigations

Definition

A personnel security investigation, also known as a PSI, is an inquiry that is made by an authorized investigative agency into an individual's activities for the purpose of making a personnel security determination. The DoD uses the PSI as the standard for the uniform collection of relevant and important information about an individual, which can be used to make a determination about his or her honesty, reliability, character, loyalty, and trustworthiness. As a security professional, you will be expected to know what a PSI is, and how it is conducted, processed, and protected.

Purpose

Personnel security investigations (PSIs) are used to determine the eligibility of an individual for access to classified information, acceptance into or retention in the Armed Forces, assignment or retention to sensitive duties or other designated duties requiring investigation. PSIs are also known as national security background investigations.

DoD military and civilian personnel, contract employees, consultants, and other persons affiliated with DoD are all subject to personnel security investigations as the basis for security determinations. Only designated individuals are authorized to request an investigation. Likewise, even fewer selected individuals are authorized to waive the investigative requirements for a PSI.

Request a PSI

To conserve investigative resources and prevent unnecessary investigations, the following guidelines have been established for requesting a PSI.

- Limit PSI requests to only those personnel who are essential to current operations.

- Limit PSI requests on military personnel to those individuals with sufficient time left in the service to warrant conducting the investigation.
- Complete all request forms and required documentation properly and in accordance with instructions.
- Government personnel submit their e-QIP to the National Background Investigations Bureau (NBIB), whereby Industry submits their request through Personnel Security Management Office for Industry (PSMO-I).
- Limit access through strict need-to-know.
- Keep priority case requests to a minimum.

Note that only authorized individuals may request a PSI.

Authorized Individuals

The list of individuals authorized to request a PSI is shown here.

- Military Departments
  - Activity commanders (Army and Air Force)
  - Commanders and commanding officers of organizations listed on the Standard Navy Distribution List (Navy, including Marine Corps)
  - Assistant Chief of Staff for Intelligence (Air Force)
  - Chiefs of recruiting stations
  - DoD Consolidated Adjudications Facility
- Defense Agencies
  - Directors of Security and activity commanders
- Organization of the Joint Chiefs of Staff
  - Chief, Security Division
- Office of the Secretary of Defense
  - Director for Personnel and Security, Washington Headquarters Services.
- Commanders of Unified and Specified Commands or their designees
- Such other requesters approved by the Deputy Under Secretary of Defense for Policy

Notice that the DoD Consolidated Adjudications Facility (DoD CAF) is included on this list. The DoD CAF makes eligibility determinations and frequently requires added investigations to come to a decision.

Waive Investigative Requirements

The individuals authorized to waive investigative requirements for sensitive positions, access to classified information, and access to Sensitive Compartmented Information (SCI) are shown here.

- For sensitive positions or access to classified information
  - Contractor personnel
    - Director, Counterintelligence and Security Programs
    - Office of the Deputy Assistant Secretary of Defense (Intelligence & Security)
    - Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
    - Deputy General Counsel, Office of General Counsel, Office of Secretary of Defense
  - Military and/or civilian personnel
    - Commander and/or agency head
    - Head of the component
    - Adjudicative authority
- For access to SCI
  - Cognizant Senior Officials of the Intelligence Community (SOICs), or their designees

Note that these are the same individuals who are authorized to suspend access to classified information.

Personal Information

Obtaining personal information about an individual's background is what a personnel security investigation (PSI) is about. All of the information that is collected is considered when making a determination of eligibility. Eligibility could be for access to classified information, assignment to a national security sensitive position, or entry or retention in the military service.

Personal information is collected in several different ways. These include having the person fill out a form, respond to questions in writing, or speak directly with the investigator. Investigators may also obtain releases from the individual for access to information that is personal. They may investigate records or interview personal references or other sources. And in certain circumstances, they may also conduct polygraph investigations, which carry some restrictions.

When someone is being processed for a security clearance eligibility, the first thing they do is complete a security questionnaire. The questionnaire used for this purpose is the Standard Form 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. Based on the outcome of the investigation, the investigator generates a report upon which an eligibility determination will be made.

Investigative Report

A report of an investigation, which includes information from many different personal sources, as well as records, allows adjudicators to get a comprehensive view of the individual. This allows the adjudicators to make a sound decision regarding the person's suitability for a position of trust, eligibility for access to classified information, and entry or retention in the military or government service.

In accordance with Executive Order 13467, the revised Federal Investigative Standards (FIS), a new five-tiered investigative model, was developed. The FIS established standard requirements for conducting background investigations for determining eligibility for access to classified information or to hold a national security sensitive position, suitability/fitness for Federal Government employment, and eligibility for logical and physical access to Federal Government controlled facilities and information systems which uses HSPD-12 credentialing. The new revised investigative standards were approved by the Security and Suitability Executive Agents in 2012 and are being implemented in phases with final implementation for all tiers scheduled by October 2017.

PSI Types

Per the FIS there are now only two background investigations approved for the initial issuance of a national security clearance eligibility or assignment to a national security sensitive position. They are the Tier 3 and Tier 5. Additionally, the Tier 3 Reinvestigation (T3R) and the Tier 5 Reinvestigation (T5R) are the new national security background investigations (PSIs) used to make continued clearance eligibility or continued assignment to a national security sensitive position determinations.

It is important to note that per the revised FIS, periodic reinvestigations for both Tier 3 and Tier 5 are required every five years. However, due to the background investigation backlog, the Tier 3 five-year reinvestigation cycle will not be implemented by the Oct 2017 timeline.

DoD, with Security Executive Agent endorsement, will delay the timeline for Tier 3 reinvestigations and increase the timeline for Tier 5 reinvestigations. The DoD timeline for periodic reinvestigations for Tier 3 will be scheduled every 10 years, while the timeline for Tier 5 reinvestigations will increase to six years. It is important to note that the Tier 5 reinvestigation six-year timeframe will be reevaluated by DoD in Dec 2017.

Please view the DoD Memorandum "Extension of Periodic Reinvestigation Timelines to Address the Background Investigation Backlog", dated January 17, 2017, from the Course Resources page for specific guidance. The other new tiered investigations are used to support suitability, public trust, and/or HSPD-12 determinations.

If you would like to know more information about the FIS implementation timelines, and compare all new and prior Federal background investigations, please see the 2012 Revised Federal Investigative Standards Crosswalk which can also be accessed from the Course Resources page.

Initial National Security Background Investigations

Tier 5 Background Investigation

Military, Contractors, and Civilians:

- Special-Sensitive positions
- Critical-Sensitive positions
- Top Secret and SCI clearance eligibility

Tier 3 Background Investigation

Military, Contractors, and Civilians:

- Noncritical-Sensitive positions
- Confidential and Secret clearance eligibility
- Military Accessions

National Security Periodic Reinvestigations

Tier 5 Reinvestigation

Military, Contractors, and Civilians:

- Special-Sensitive positions
- Critical-Sensitive positions
- Top Secret or SCI clearance eligibility

Tier 3 Reinvestigation

Military, Contractors, and Civilians:

- Noncritical-Sensitive positions
- Secret or Confidential clearance eligibility reinvestigation

Prior National Security Initial and Periodic Background Investigations

Single Scope Background Investigation (SSBI)

Military, Contractors, and Civilians:

- Special-Sensitive positions
- Critical-Sensitive positions
- Top Secret and SCI clearance eligibility

Access National Agency Check and Inquiries (ANACI)

Civilians:

- Non Critical-Sensitive positions
- Secret or Confidential clearance eligibility

National Agency Check with Law and Credit Check (NACLC)

Military and Contractors:

- Secret or Confidential clearance eligibility
- All military accessions and appointments

Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)

Military, Contractors, and Civilians:

- Special-Sensitive positions
- Critical-Sensitive positions
- Top Secret and SCI clearance eligibility

Phased Periodic Reinvestigation (PPR)

Military, Contractors, and Civilians:

- Same as SSBI-PR but more efficient
- **Phase 1:** determines whether Phase 2 is necessary
- **Phase 2:** only performed if Phase 1 yields issue-relevant information

National Agency Check with Law and Credit Check (NACLC)

Military, Contractors, and Civilians:

- Non Critical-Sensitive
- Secret or Confidential clearance eligibility reinvestigation

Information Advisement to Subject

One provision of the Privacy Act of 1974 is that when an agent of the federal government gathers personal information from an individual, that individual must be advised of four points.

- Under what authority is the information being gathered?
- What is the principal purpose for gathering the information?

- How will the information routinely be used?
- Is providing the information mandatory or voluntary, and what are the potential consequences of refusing to provide information?

If the individual who is being investigated refuses to provide information or sign a release that will be used to gather information, the processing may be halted at that time. If the individual currently has a security clearance or is assigned to other sensitive duties, then the CAF could start action to revoke the individual's security eligibility. A Privacy Act Advisement is given each and every time information is collected from an individual during the investigation. When personal information is required to fill out a form, the advisement usually is printed on the form.

Investigative Agency

The investigative agency that has responsibility for conducting background investigations for the Department of Defense is the National Background Investigations Bureau, also known as NBIB, which is housed at the Office of Personnel Management (OPM).

Record Keeping

A final consideration in the PSI process is how the resultant personnel records are to be handled and stored. Who is responsible for safeguarding PSI records? Who has access to PSI records? Where are PSI records stored, and how are they disposed of?

Responsibility for PSI Records

Responsibility for safeguarding PSI records rests with the DoD authorities who administer the DoD personnel security program and all DoD personnel who are authorized to have access to such records. To ensure that PSI information is used only for official and authorized purposes, DoD Components must have in place a system of internal controls to protect records from unauthorized access or disclosure and to preserve confidentiality.

There are several procedures to safeguard PSI reports and other personnel security records. First, the authorized requester is responsible for control and accountability of any reports it receives. Second, the reproduction of PSI reports is restricted to the minimum number of copies required to perform official duties. Third, PSI reports must be stored in a secured container, such as a vault or safe. Fourth, PSI reports must be sealed in double envelopes when being transmitted by mail or courier. And finally, any information regarding an individual's personnel security clearance status must be protected.

Access to PSI Records

To protect the fundamental right to privacy of individuals under investigation, access to PSI records and information is limited to only those whose official duties require access

to such information. Outside of the DoD, PSI reports may be released only with the specific approval of the investigative agency with authority over the reports. Within the DoD, access to PSI reports is limited to only those designated DoD officials who require access for official personnel security duties. Subjects of PSIs also may have access to PSI 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. Information about personnel security clearance eligibility determinations is restricted to DoD and other federal government officials with an official need to know.

Disposition and Destruction of PSI Records

The disposition and destruction of PSI records are subject to strict regulations. DoD recipient organizations requesting PSI reports may retain them for only the time necessary to fulfill the originally requested official purpose. These reports are the property of the investigating organization and are provided to the requesting organization as a loan.

Official PSI reports are stored in DoD records repositories that are authorized to store PSI reports. Favorable reports are destroyed after 15 years. Reports of a minor derogatory nature are also destroyed after 15 years. And reports resulting in unfavorable administrative action or court-martial are destroyed after 25 years. Sometimes PSIs are conducted on individuals who are being considered for DoD affiliation but never complete their affiliation. These PSI reports are destroyed after one year. PSI reports must be destroyed in the same manner that is used for the destruction of classified information.

Summary

In this section you learned that a personnel security investigation is an inquiry made by an authorized investigative agency into an individual's activities for the purpose of making a personnel security determination. DoD uses the PSI as the standard for the uniform collection of relevant information about an individual. A PSI contains personal information that is collected via records reviews and personal interviews, as well as information that the applicant provides by filling out a questionnaire.

The subject of an investigation is required to sign a release that will allow an investigator to access all necessary information to compile a comprehensive report. In accordance with provisions of the Privacy Act of 1974, whenever an investigator speaks with a subject of an investigation, the subject is informed of the authority for the investigation, the principal purpose of gathering the information, the routine uses of the information, and the voluntary or mandatory nature of the disclosure, including the possible consequences of not providing information. The NBIB is the investigative agency that conducts personnel security investigations for the Department of Defense. As you can see, the PSI is very involved, and serves several purposes.

Review Activity: Personnel Security Investigations

Which of the following does the DoD use as the standard for the uniform collection of relevant and important information about an individual?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Access
- ○ PSI
- ○ Release
- ○ Privacy Act

Which of the following is the name of the advisement that an investigator is required to give the subject each time that information is requested from them?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Access
- ○ PSI
- ○ Release
- ○ Privacy Act

For which of the following are Personal Security Investigations used to determine?

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

- ☐ Access to classified information
- ☐ Acceptance or retention to the armed forces
- ☐ Assignment or retention to sensitive positions

Military Special Requirements

Overview

Several special conditions and requirements exist for military personnel and retirees. All individuals applying for entry into the U.S. Armed Forces must meet the military service standard, which is the standard that is applied in determining whether a person is eligible for appointment, enlistment, induction, or retention in the Armed Forces. At its most basic level, it is the standard that is used to conclude that no reasonable basis exists for doubting a person's loyalty to the U.S. government. Other special considerations include investigative requirements for military personnel and access to classified information by retired flag or general officers.

Investigative Requirements

All military personnel are subject to specific investigative requirements upon enlistment, appointment, or reentry to the service.

As you will recall, the Tier 3 is conducted for all military personnel upon initial entry into the Armed Forces, unless the position requires access to Top Secret information or SCI, in which case a Tier 5 investigation must be conducted. A Tier 3 is conducted upon reentry to the Armed Forces following a gap in service of more than 24 months.

As with most rules, there are some exceptions. For example, some commissioned officers of Reserve components, including healthcare professionals, chaplains, and attorneys, may be commissioned prior to completion of the PSI. In such circumstances, the PSI must be initiated when the application for commission is received. Furthermore, the applicant is subject to discharge if the investigation results in an unfavorable outcome that leads the military to conclude that the applicant is not eligible to hold a commission. Another exception is in regard to the mobilization of military retirees. In the event of full or partial mobilization of retired military personnel, the requirement for a reentry investigation can be waived. Further priority is given to those who are assigned to defense intelligence and security agencies. Finally, if an active duty flag or general officer finds compelling reasons to grant classified access to a retired flag or general officer for 90 days or less, then the requirement for investigation can be waived.

Access for Retired Flag/General Officers

Certain conditions and restrictions apply when access to classified information is granted to retired flag or general officers. As mentioned previously, the investigative requirement for access to classified information may be waived for a retired flag or general officer if an active duty flag or general officer has a compelling reason for that individual to have access. Such access is limited to 90 days or less and to information classified at a level commensurate with the security clearance held at the time of retirement. Access to retired flag or general officers may be granted only after the reason for the access and

the purpose of the associated DoD mission have been detailed. In addition, access may be granted only under the condition that the classified materials are not removed from their approved storage area. When granting access to retired flag or general officers, the active duty officer who approved the clearance must provide the DoD with a written record containing full identification details of the cleared individual and the classification level of the information for which the access was granted.

Other Types of Access

Overview

In a few specialized cases, access to classified information may be granted before a security clearance eligibility is complete. In this section, we are going to discuss interim eligibility and one-time access.

Interim Eligibility

In this section, we are going to take a brief look at what an interim eligibility is. If an individual is needed to work on a specific project before his or her background investigation and adjudication has been completed, local commands or other authorities have the option of granting an interim clearance. Interim eligibility allows employees to begin working on sensitive or classified projects until a final security clearance eligibility is granted or denied.

Not all employees are eligible for an interim eligibility. Prior to granting the interim eligibility, a favorably reviewed SF-86 must be submitted and the proper investigation opened by the investigative service provider. Additionally, there are certain requirements that must be met before an interim eligibility can be granted. Section 7.16 of the DoD Manual 5200.02 outlines the specific requirements.

One-Time Access

Like interim eligibility, one-time access allows personnel to access information without a full security upgrade. One-time access may be granted to DoD personnel if they have an existing clearance eligibility but require short-term access to classified information at a higher level than currently authorized, and if the processing time required to upgrade the clearance eligibility would preclude timely access to the information. This can happen when someone has Secret clearance eligibility and needs access to Top Secret information due to an urgent operational or contractual situation. However, this should only be done sparingly.

Review Activities: Other Types of Access

For each statement, select True or False. Check your answers in the Answer Key at the end of this Student Guide.

Statement 1 of 5. The CAF is the only authority who can grant an interim eligibility

- ○ True
- ○ False

Statement 2 of 5. An interim eligibility is granted on a temporary basis.

- ○ True
- ○ False

Statement 3 of 5. All applicants are authorized for an interim eligibility.

- ○ True
- ○ False

Statement 4 of 5. The requirements for granting an interim eligibility are:

a. No need for immediate access
b. SF86 submitted and investigation opened by ISP
c. All minimum requirements for interim eligibility satisfied

- ○ True
- ○ False

Statement 5 of 5. One-time access lasts indefinitely.

- ○ True
- ○ False

DoD CAF

Overview

Welcome to a brief introduction to the DoD Consolidated Adjudications Facility, also referred to as DoD CAF. As a security professional, you will often hear this acronym. It is likely that you will interact with at least one of these facilities during the course of your security career. The CAF has many responsibilities. They include making national security adjudicative decisions, being a central repository for investigative records, and requesting additional information where there is evidence that someone may no longer be eligible for a clearance.

The DoD CAF makes eligibility determinations by applying the national security adjudicative guidelines and the "whole person concept." The final decision is a balance of interests for national security against the interests of the individual. When an individual's loyalty, trustworthiness, or reliability is in question, the decision is always made in favor of national security.

In the future, you will learn much more about the CAF's role and responsibilities within the DoD Personnel Security Program.

National Security Adjudicative Decisions

Ultimately, national security adjudicative decisions will result in a security clearance eligibility being either granted or denied. In cases in which an individual has already been granted a security clearance eligibility, the eligibility may be revoked or terminated based upon new information that arises during re-adjudication. The revocation or termination of a favorable eligibility security clearance determination could lead to the termination of DoD civilian employment if an individual's employment was based on their security clearance eligibility. In such cases, an individual may be restored to duty at the discretion of the head of the DoD component. Security clearance eligibility upgrades are requested when an individual has a need for a higher level of eligibility. Likewise, security clearance eligibility downgrades occur when an individual no longer has a need for a higher level eligibility but still requires a lower level eligibility.

Review Activity: DoD CAF

Joe needs to conduct a brown bag meeting about the DoD CAF as an annual requirement. For his presentation, he needs to identify all the responsibilities of the DoD CAF.

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

- ☐ Makes national security adjudicative decisions
- ☐ Performs personnel security investigations
- ☐ Is a central repository for investigative records
- ☐ Requests additional information where there is evidence that someone may not maintain a security clearance eligibility

Adjudicative Process

Overview

This section will provide you with a brief overview of the adjudicative process. As your career in the security field progresses, you will learn much more about adjudication.

The adjudicative process begins once a personnel security investigation is complete, and a report of investigation has been submitted. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. The adjudicative process is the careful weighing of a number of variables, known as the whole person concept.

All available, reliable information about the person, past and present, favorable and unfavorable, is considered in reaching a final determination. 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. This is where the whole person concept is applied. 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.

Some examples include Sensitive Compartmented Information, presidential support, and various nuclear programs. Another type of adjudicative decision is when a local command determines an individual's trustworthiness for a position that does not require access to classified information or is not a sensitive position. Some examples include access to unclassified DoD information systems, facilities, and other positions of trust.

Review Activity: Adjudicative Process

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

Statement 1 of 4. This local person can make a trustworthy determination

- ○ Commander
- ○ Whole person
- ○ Advisement
- ○ ROI

Statement 2 of 4. Provided to subject during information collection

- ○ Commander
- ○ Whole person
- ○ Advisement
- ○ ROI

Statement 3 of 4. The name of the concept that is applied by an adjudicator when reviewing investigations

- ○ Commander
- ○ Whole person
- ○ Advisement
- ○ ROI

Statement 4 of 4. The report submitted that begins the adjudicative phase

- ○ Commander
- ○ Whole person
- ○ Advisement
- ○ ROI

Adjudicative Guidelines

Overview

This section lesson provides a quick look at the guidelines an adjudicator follows during the adjudication process.

The Director of National Intelligence Security Executive Agent Directive, or DNI SEAD, 4 provides adjudicative guidelines for determining eligibility for access to classified information or assignment to sensitive duties. Ultimately, security clearance eligibility must be clearly consistent with the interests of national security. The decision to grant or continue eligibility must be an overall common sense determination based upon careful consideration of the following:

- 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
- Use of information technology

Each of the foregoing is evaluated in the context of the whole person.

Review Activity: Adjudicative Guidelines

What does the DNI SEAD 4 provide for determining access to classified information or assignment to sensitive duties?

Think of your answer then check the Answer Key at the end of this Student Guide.

What concept do adjudicators use when applying the adjudicative guidelines?

Think of your answer then check the Answer Key at the end of this Student Guide.

Continuous Evaluation

Overview

There is a clear need to assure the ongoing trustworthiness of an individual, even after a personnel security determination has been reached. Therefore the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and co-worker, and, to a large degree, the individual. Each DoD component has a program designed to continually evaluate, on a continuing basis, the status of personnel with respect to security eligibility. Close coordination between security authorities and personnel, medical, legal, and supervisory personnel is necessary to assure that all pertinent information is considered in the personnel security process.

Continuous Evaluation Process

All individuals who hold a security clearance eligibility are subject to continuous evaluation. Continuous evaluation is the uninterrupted assessment of an individual for retention of a security clearance eligibility, or a continuing assignment to sensitive duties. It is the responsibility of all security personnel to continuously evaluate personnel assigned to their command or activity. Anyone who becomes aware of information that might make an individual ineligible for a security clearance must report this information to his or her supervisor or to a local security official. Supervisors, coworkers, and individuals themselves all have an obligation to report potentially disqualifying information. The ultimate responsibility for maintaining continued security clearance eligibility rests with the individual. Periodic reinvestigations are conducted as part of the process of continuous evaluation. Additionally, continuous evaluation will also incorporate an automated records check monitoring system which will cover the gap between initial and periodic reinvestigations in the near future.

Summary

To quickly review the information, recall that continuous evaluation is a process that enables security professionals to monitor individuals who maintain security clearance eligibility. Relevant information should be received from security authorities, medical, legal, and supervisory personnel, and the individuals themselves. Periodic reinvestigations are a part of this process.

Review Activity: Continuous Evaluation

Review the following memo and identify the errors. When finished, check your answers in the Answer Key at the end of this Student Guide.

MEMO: To all employees
FROM: Joe Smith, Director of Security

First of all I would like to thank all of you for your hard work and dedication to our security programs. Just as an annual refresher I would like to review the continuous evaluation process.

It is the responsibility of this office to maintain the continuous evaluation of personnel with security clearance eligibility. It is important that we not pay close attention to individuals with security clearances because we don't want individuals to think that we are spying on them.

The continuous evaluation process is the uninterrupted assessment of an individual for retention of a job, or a continuing assignment to sensitive duties.

When an individual has a security clearance eligibility, information on that individual is rarely checked due to all of the other duties we have. We expect that if they have a clearance they will not do anything that would bring attention to themselves or their agency.

Once a person is granted a security clearance eligibility, they are no longer subject to an investigation.

I hope that all of this information has been helpful. Please do not hesitate to contact me if you need further clarification concerning the continuous evaluation process.

Have a great day!

Course Lessons Review

This concludes the Introduction to Personnel Security course. Here is a list of the lessons in the course.

- Lesson 1: Personnel Security Policy
- Lesson 2: DoD Personnel Security Program
- Lesson 3: Security Clearance Eligibility Process

Course Objectives

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

- ✓ Identify the purpose of personnel security
- ✓ Identify the history of personnel security
- ✓ Identify policy documents

- ✓ Describe the authority that establishes the DoD Personnel Security Program
- ✓ Describe the five elements of the Personnel Security Program
- ✓ Explain access to sensitive duties
- ✓ Explain requirements of sensitive duties
- ✓ Explain civilian personnel designations
- ✓ Identify special access programs

- ✓ Describe security office duties, briefings, and the e-QIP system
- ✓ Answer the following questions:
    - o What is a security clearance eligibility?
    - o How is a security clearance eligibility processed?
    - o How is a security clearance eligibility granted?
- ✓ Identify
    - o Restrictions
    - o Access
    - o Personnel Security Investigations (PSIs)
    - o Need-to-Know
    - o The Privacy Act of 1974
    - o Electronic Questionnaire for Investigative Processing (e-QIP)
    - o Definition and purpose of a PSI
    - o Personal information
    - o Types of PSIs
    - o The information advisement
    - o Investigative agency
    - o Interim clearances

Congratulations

Congratulations! You have completed the *Introduction to Personnel Security, v4* course.

To receive course credit, you must take the *Introduction to Personnel Security, v4* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 1 Review Activity

Review Activity: Personnel Security Policy

Terms:

A. Spoils System

B. E.O. 10450

C. DoDI 5200.02

D. Loyal, trustworthy, reliable

E. Civil Service Commission

F. Hatch Act, 1939

Descriptions:

__D__ Character traits looked for in a government employee

__A__ System that required allegiance to a political party and not the Constitution

__E__ The Civil Service Act of 1883 created this

__F__ Act that represents the beginning of the Personnel Security Program

__B__ The Executive Order that managed federal civilian employees

__C__ DoD instruction that establishes the policy, assigns responsibilities, and prescribes procedures for the DoD Personnel Security Program

Lesson 2 Review Activities

Review Activity: DoD Personnel Security Program

Terms:

A. Continuous Evaluation

B. Reinvestigation

C. Adjudication

D. Investigation

E. Designation

Descriptions:

__E__ An assessment of a position's potential impact on the national security is a part of this process.

__C__ A judgment concerning security clearance eligibility is made by evaluating the information in the PSI with DoD standards.

__B__ This is part of the CEP. It is done at certain intervals based on duties or access.

__D__ A report is generated from this that contains information about an individual who has been selected for special duties. The report is used to evaluate the individual for eligibility.

__A__ This is used to monitor employees for new information or changes that could affect their status.

Review Activity: Sensitive Duties

Question 1 of 6. The majority of Joe's employees are civilians who work on very sensitive projects that require access to Top Secret information. These civilian employee positions are categorized as which of the following?

- ○ Non-Critical Sensitive
- ⊙ Critical Sensitive *(correct response)*
- ○ Special Sensitive

Question 2 of 6. Two civilians who require access to Sensitive Compartmented Information have position sensitivity categories of which of the following?

- ○ Non-Critical Sensitive
- ○ Critical Sensitive
- ⊙ Special Sensitive *(correct response)*

Question 3 of 6. Most military personnel who work in the office must have *(fill in the blank)* to classified information at the Top Secret or Secret level in the official performance of their duties.

- ⊙ Access *(correct response)*
- ○ Limited Access Authorization

Question 4 of 6. The Comptroller of the base also reports to Joe. This person's civilian position is categorized as Critical Sensitive due to fiduciary duties requiring procurement of services in excess of (fill in the blank).

- ○ $500,000
- ○ $500 million
- ⊙ $50 million *(correct response)*

Question 5 of 6. He also has a few employees who develop and deliver instruction to other DoD employees at the agency. Their duties are sensitive and could potentially damage national security if information was leaked; however, the information would not be as harmful as that from a Critical Sensitive designation. Which designator do these individuals have?

- ○ Public Trust
- ⊙ Non-Critical Sensitive *(correct response)*
- ○ Special Sensitive

Question 6 of 6. Joe also has an individual on temporary assignment working in his office. He is a member of the Royal Navy, and as such is a British citizen. In the position he is filling, it is not possible or not practical to use a U.S. citizen. For this reason, he has been granted which of the following?

- ○ Access
- ○ Clearance
- ⊙ Limited Access Authorization *(correct response)*

Review Activity: Special Access Requirements

Question 1 of 2. Special access requirements are designed to provide an additional layer of security to some of our nation's most valuable assets.

- ⦿ True *(correct response)*
- ○ False

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

Question 2 of 2. Having an active security clearance eligibility makes one eligible to access all classified information.

- ○ True
- ⦿ False *(correct response)*

Feedback: *Having an active security clearance eligibility does NOT make one eligible to access all classified information.*

Review Activity: Security Office

Which of the following are security office duties?

- ☑ set date to conduct an annual briefing *(correct response)*
- ☑ evaluate Mr. Jones's interim eligibility paperwork *(correct response)*
- ☑ call the medical office about Ms. May *(correct response)*
- ☑ request personnel security investigation for new employee *(correct response)*
- ☑ call Mr. Carpenter and assist him with his e-QIP *(correct response)*
- ☐ plan the holiday party for the security office
- ☐ order cleaning supplies
- ☑ set a date to conduct training on personnel security requirements *(correct response)*

Lesson 3 Review Activities

Review Activity: Security Clearance Eligibility Process

Question 1 of 4. Joe Smith received an unfavorable security clearance eligibility determination for his security clearance. He is now able to go and work on the classified project that he has wanted to work on.

- ○ Fact
- ⊙ Fiction *(correct response)*

Question 2 of 4. The Department of Defense does not define regular access in terms of specific time periods. Joe could need access just once a week or even monthly and that could be defined as regular access.

- ⊙ Fact *(correct response)*
- ○ Fiction

Question 3 of 4. The first phase of the security clearance eligibility process is the personnel security investigation.

- ⊙ Fact *(correct response)*
- ○ Fiction

Question 4 of 4. Even though Mr. Curly is a citizen of Germany he will be able to have access to any classified information anywhere once he has obtained his Limited Access Authorization (LAA).

- ○ Fact
- ⊙ Fiction *(correct response)*

Review Activity: Key Concepts

When the federal Government collects personal information from an individual, it is required that the individual be informed of which of the following?

- ☑ Under what authority the Government agent is collecting the information *(correct response)*
- ☑ The purpose for collecting the information *(correct response)*
- ☑ The routine uses of the information *(correct response)*
- ☑ Whether providing this information is voluntary or mandatory *(correct response)*

Review Activity: Clearance Software

Question 1 of 4. What system does Mr. Smith need to access when he needs to update his personal information prior to a reinvestigation?

- ⦿ e-QIP *(correct response)*
- ○ JPAS
- ○ JCAVS
- ○ JAMS

Question 2 of 4. If Mr. Smith's security manager needs to communicate with a CAF he would use what system?

- ○ e-QIP
- ○ JPAS
- ⦿ JCAVS *(correct response)*
- ○ JAMS

Question 3 of 4. JCAVS and what other sub-system make-up the JPAS system?

- ○ e-QIP
- ○ JPAS
- ○ JCAVS
- ⦿ JAMS *(correct response)*

Question 4 of 4. Which system is the Department of Defense system that uses the Web to connect security personnel around the world?

- ○ e-QIP
- ⦿ JPAS *(correct response)*
- ○ JCAVS
- ○ JAMS

Review Activity: Personnel Security Investigations

Which of the following does the DoD use as the standard for the uniform collection of relevant and important information about an individual?

- ○ Access
- ⦿ PSI *(correct response)*
- ○ Release
- ○ Privacy Act

Which of the following is the name of the advisement that an investigator is required to give the subject each time that information is requested from them?

- ○ Access
- ○ PSI
- ⊙ Release *(correct response)*
- ○ Privacy Act

For which of the following are Personal Security Investigations used to determine?

- ☑ Access to classified information *(correct response)*
- ☑ Acceptance or retention to the armed forces *(correct response)*
- ☑ Assignment or retention to sensitive positions *(correct response)*

Review Activity: Other Types of Access

Statement 1 of 5. The CAF is the only authority who can grant an interim eligibility.

- ○ True
- ⊙ False *(correct response)*

Feedback: *Interim eligibility is granted by local commands or other authorities (not ONLY the DoD CAF).*

Statement 2 of 5. An interim eligibility is granted on a temporary basis.

- ⊙ True *(correct response)*
- ○ False

Feedback: *True as stated.*

Statement 3 of 5. All applicants are authorized for an interim eligibility.

- ○ True
- ⊙ False *(correct response)*

Feedback: *Applicants for security clearance eligibility may not be granted an interim eligibility if unresolved issues exist.*

Statement 4 of 5. The requirements for granting an interim eligibility are:

a. No need for immediate access
b. SF86 submitted and investigation opened by ISP
c. All minimum requirements for interim eligibility satisfied

- ⦿ True *(correct response)*
- ○ False

Feedback: *True as stated.*

Statement 5 of 5. One-time access lasts indefinitely.

- ○ True
- ⦿ False *(correct response)*

Feedback: *One-time access grants access for a short duration only.*

Review Activity: DoD CAF

Joe needs to conduct a brown bag meeting about the DoD CAF as an annual requirement. For his presentation, he needs to identify all the responsibilities of the DoD CAF.

- ☑ Makes national security adjudicative decisions *(correct response)*
- ☐ Performs personnel security investigations
- ☑ Is a central repository for investigative records *(correct response)*
- ☑ Requests additional information where there is evidence that someone may not maintain a security clearance eligibility *(correct response)*

Feedback: *The DoD CAF is responsible for all of these tasks except for performing personnel security investigations which is the responsibility of NBIB or other investigative service providers.*

Review Activity: Adjudicative Process

Statement 1 of 4. This local person can make a trustworthy determination

- ○ Whole Person
- ⦿ Commander *(correct response)*
- ○ Advisement
- ○ ROI

Statement 2 of 4. Provided to subject during information collection

- ⦿ Advisement *(correct response)*
- ○ Whole person
- ○ Commander
- ○ ROI

Statement 3 of 4. The name of the concept that is applied by an adjudicator when reviewing investigations

- ○ Commander
- ○ Advisement
- ⦿ Whole Person *(correct response)*
- ○ ROI

Statement 4 of 4. The report submitted that begins the adjudicative phase

- ○ Commander
- ○ Whole person
- ○ Advisement
- ⦿ ROI *(correct response)*

Review Activity: Adjudicative Guidelines

What does the DNI SEAD 4 provide for determining access to classified information or assignment to sensitive duties?

Answer: adjudicative guidelines

What concept do adjudicators use when applying the adjudicative guidelines?

Answer: whole person

Review Activity: Continuous Evaluation

MEMO: To all employees
FROM: Joe Smith, Director of Security

First of all I would like to thank all of you for your hard work and dedication to our security programs. Just as an annual refresher I would like to review the continuous evaluation process.

It is the responsibility of this office to maintain the continuous evaluation of personnel with security clearance eligibility. **It is important that we not pay close attention to individuals with security clearances because we don't want individuals to think that we are spying on them.**

The continuous evaluation process is the uninterrupted assessment of an individual for retention of a **job**, or a continuing assignment to sensitive duties.

When an individual has a security clearance eligibility, information on that individual is **rarely checked due to all of the other duties we have. We expect that if they have a clearance they will not do anything that would bring attention to themselves or their agency.**

Once a person is granted a security clearance eligibility, they are **no longer subject to an investigation.**

I hope that all of this information has been helpful. Please do not hesitate to contact me if you need further clarification concerning the continuous evaluation process.

Have a great day!

Error 1: *"It is important that we not pay close attention to individuals with security clearances because we don't want individuals to think that we are spying on them."*

Feedback: *The purpose of continuing to check on individuals with security clearance eligibility is to identify potential issues that may affect their security clearance eligibility.*

Error 2: *"...for retention of a job…"*

Feedback: *The continuous evaluation process is the uninterrupted assessment of an individual for the retention of a security clearance eligibility or continuous assignment to sensitive duties.*

Error 3: *"… rarely checked due to all of the other duties we have. We expect that if they have a clearance they will not do anything that would bring attention to themselves or their agency."*

Feedback: *When an individual has a security clearance eligibility, information on that individual is monitored continuously.*

Error 4: *"…no longer subject to an investigation."*

Feedback: *Once a person is granted a security clearance eligibility, they are subject to periodic reinvestigations.*