



**Personnel Security
Adjudications
Independent Study Course
PS001.08**

Security through Knowledge

Defense Security Service Academy
938 Elkridge Landing Road, Linthicum, MD 21090
DSN 283-7295 – (410) 865-2295
<http://www.dss.mil/training>



Personnel Security Team

LESSON 2

The Employing Activities' Initial Responsibilities

In this Lesson we will look at some of the responsibilities of the employing activity as they pertain to the Personnel Security Program. They involve the determination that a personnel security investigation is needed, who may request it, and the requirements for granting interim security clearances and how Special Access Programs (SAPs) are structured. The employing activities must fulfill their mission by using qualified personnel to perform the mission.

We will address the military and civilian position requirements, standards and designations. You will see what the position sensitivity levels are and the activity's responsibility for identifying sensitive positions which require certain types of PSIs.

After identifying the position sensitivity levels and their requirements, we will discuss the role of the Employing Activity as it pertains to the accomplishment of the DoD mission. One important function of the employing activity is determining trustworthiness for access to classified information.

Also, we will look at the requesting procedures for PSIs, and those individuals who are authorized to originate and request them after it has been determined that the need exists.

What authorities are authorized to grant an Interim security clearance? We will find the answer to that question as well as identify the restrictions and requirements that apply to Interim clearances.

One-time access, emergency appointments and their relationship to Interim clearances will be discussed also.

Finally, you will learn about Special Access Programs (SAPs), their structure, design and what DoD regulation governs them, as well as what special investigative requirements pertain to SAPs. Continuous evaluation will also be addressed.

OBJECTIVES

At the end of this lesson you should be able to do the following:

- * Identify the regulation that applies to civilian position sensitivity designations.
- * Identify the levels of position sensitivity.
- * Define the responsibilities of the employing activity within the personnel security program.
- * State how an employing activity obtains a trustworthiness determination on individuals occupying sensitive positions.
- * State who is authorized to originate the request for an investigation.
- * Define an Interim Clearance and what restrictions apply.
- * State the Personnel Security Investigations requirements for Special Access Programs.

READING ASSIGNMENTS

Assignments 1:

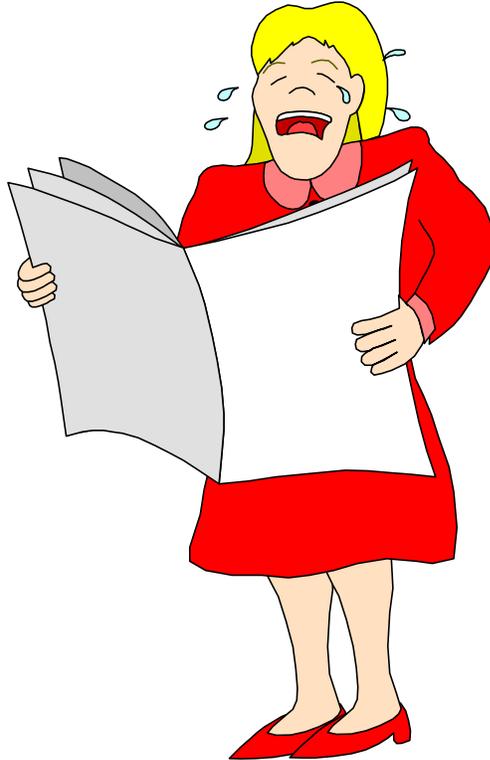
DoD 5200.2R: Chapter 2, Para 2-101 to 2-102

DoD 5200.2R: Chapter 3, Para.3-100 to 3-102

DoD 5200.2R: Chapter 5

DoD 5200.2R: Chapter 7

DoD 5200.2R: Appendix F: Para.A



DESIGNATING SENSITIVE DUTIES

In this lesson we will look at the military and civilian position requirements, standards, and their designations. You will see the levels of sensitivity, the clearance and sensitive position standards, the reasons why a position is designated as sensitive, the command's responsibility for identifying sensitive positions, and the personnel security investigations required.

Let's start with the civilian positions first.

CIVILIAN POSITION SENSITIVITY LEVELS

One of the most important aspects of personnel security is determining the sensitivity of the material to which the incumbent of a position must have access to perform his/her official duties. The sensitivity then determines the extent of investigation which must be conducted to provide the minimum risk to the material.

Within the Executive Branch, E.O. 10450 establishes the civilian sensitive position program. The Federal Personnel Manual then defines the levels of sensitivity for civilian positions within the federal government. DoD 5200.2-R establishes the Personnel Security Program within DoD and provides criteria for evaluating the sensitivity level of civilian positions. The same criteria are additionally used to determine sensitive duty levels for military and contractor personnel.

The levels of sensitivity used in DoD are:

- Nonsensitive
- Noncritical-sensitive
- Critical-sensitive

***DoD has three
sensitivity levels***

Military personnel assigned to sensitive duties are investigated and adjudicated based on the sensitive material to which they will be exposed while performing official duties.

AUTHORITIES

The primary authorities to designate sensitive positions are shown in the reading assignment (although personnel and supervisory officials actually implement the program):

- * Heads of DoD Components or their designees for critical-sensitive positions.
- * Organizational commanders for noncritical-sensitive positions.

CRITERIA

The Civilian Personnel Officers and their staffs normally have the authority, delegated by component regulations, to make position sensitivity determinations based on the criteria in Chapter III, DoD 5200.2-R and input from principal staff officers.

The criteria to be applied in designating a position as critical-sensitive (**highest level in DoD**) include a variety of assignments as shown in your reading but the most frequent reason is access to Top Secret information.

The criteria to be applied in designating a position as noncritical-sensitive also include the variety of assignments listed in your readings but once again access to Secret or Confidential information is the most frequent justification.

Positions are designated as nonsensitive if they contain no sensitive duties.

All positions not designated critical-sensitive or non-critical sensitive are designated as nonsensitive. Therefore, the specific criteria shown in your readings are the only factors in determining critical-sensitive and noncritical-sensitive positions.

INVESTIGATIONS REQUIRED

Once the sensitivity of a position is determined, the incumbent of the position must be investigated based on the sensitivity level of the position and a trustworthiness adjudication determination made.

For assignment to a **critical-sensitive** position, a favorably adjudicated Single Scope Background Investigation (SSBI) must be conducted.

For assignment to a **noncritical-sensitive** position within DoD (civilian employees) an Access National Agency Check with Inquiries (ANACI) must be submitted.

On **military personnel**, a National Agency Check with Local Agency and Credit Checks (NACLCC) must be conducted for assignment to sensitive duties involving access to Secret or Confidential information or clearance eligibility and for appointment as a commissioned officer.

For **nonsensitive duties**, the NACI is used as a pre-employment investigation for DoD civilians and a DoD The Entrance NAC (ENTNAC) is used to support enlistment in the Armed Forces.

STANDARDS

When dealing with civilian employees or members of the Armed forces, the entire personnel security process relies upon requiring minimum standards of trustworthiness for the granting of a security clearance, assignment to sensitive duties, or access to classified information. The **Clearance and Sensitive Position Standard** applied to DoD civilian employees and the **Military Service Standard** applied to military members (stated in DoD 5200.2-R) establish levels of trustworthiness required of military and civilian employees.

Designating sensitive duties is an important part of

the PSP. The type investigation conducted and the adjudication action taken are based on the sensitivity of the duties the individual will perform. Familiarity with the process will aid the adjudicator in making valid decisions.

EMPLOYING ACTIVITIES

One of the most important roles in the Personnel Security Program is played by the employing activity. These activities have the responsibility to successfully complete the mission through the proper use of personnel assigned to them.

You will find that a basic requirement of personnel management is that after a sensitive position is designated to support the mission, the personnel assigned must be qualified to perform in the position. One aspect of qualification is insuring that an individual is trustworthy to have access to classified information or performing other sensitive duties required of the position.

We will determine why the employing activity must take the necessary actions, not only to determine trustworthiness, but to provide proper access when the trustworthiness determination has been made.

EMPLOYING ACTIVITY RESPONSIBILITIES

Who has one of the most important roles in the Personnel Security Program (PSP)? Who has the responsibility to ensure that a Personnel Security Investigation (PSI) is essential to current operations? The answer to these questions is the Employing Activity.

We will discuss the determination or prediction of a person's trustworthiness based on some form of investigation. The nature and extent of the investigation is determined by the level of clearance or the sensitivity of duties required for the employee to do the assigned job.

Employing activity determines when prerequisites have been met.

Thus, enters the employing activity. By submitting an investigative request on behalf of an employee, the employing activity is essentially saying that certain prerequisites have been met. DSS and OPM depend on the employing activity to ensure the requests for investigation packages are complete to avoid delays in processing. **(A checklist is provided in Figure 2-1)**

HOW TO AVOID DELAYS IN PROCESSING THE PSI

- Request only essential PSIs.
- Ensure, as far as possible, through a careful review that all forms are completed fully and correctly.
- Be sure to address all mailings correctly.
- Prepare and forward packages in a timely manner.

Figure 2-1

Most of the employing activities actions relating to PSIs will eventually involve the adjudicator directly. Some of these actions are:

Establishing position sensitivity

- Access to classified information required by a position assignment

Completing requests for investigation forms and supporting actions

Waiving investigative requirements on critical sensitive appointments

Interim clearances

Required security education

Adverse information reporting

Administering locally due process

The responsibility to the employee does not end with the submission of the PSI request package.

While the protection of classified information rests with the cleared employee, the employing activity has the task of educating that employee and keeping personnel security clearance related records. The personnel security clearance is not a piece of paper. It is a determination, essentially an educated guess, as to a person's character and the issuance of a clearance eligibility is not the final word on that person's character.

Issuance of a clearance eligibility is not the final word on a person's character.

The personnel security determination allows for the possibility of inaccuracy in the original determination or prediction and also for the changes in a person's character over time. In order to maintain the validity of the clearances, employing activities request periodic reinvestigations on cleared personnel.

CONTINUED COMMAND ATTENTION

Only PSIs that are essential to current operations should be requested.

The employing activity must ensure that PSIs are necessary and authorized by DoD policies. Only those PSI's that are essential to current operations should be requested. Investigations requested for clearance eligibility should be limited to those instances where an individual has a clear need for access to classified information or sensitive duties. Also, PSI's required to determine clearance eligibility must not be requested in frequency or scope which will exceed that provided for by regulation.

In view of the foregoing, the following guidelines have been developed to simplify and facilitate the investigative request process:

- Limit requests for investigations to those that are essential to current operations and clearly authorized by DoD policies and attempt to utilize individuals who, under the provisions of the regulation, have already met the security standard;
- Assure that military personnel on whom investigative requests are initiated will have sufficient time remaining in service after completion of the investigation to warrant conducting it;
- Insure that request forms and prescribed documentation are properly executed in accordance with instructions.
- Ensure that the Electronic Personnel Security Questionnaire (EPSQ), it is completely and accurately completed.
- Dispatch the request directly to DSS (PIC) and OPM (FIPC) as appropriate.

Request forms and documentation must be properly executed IAW instructions.

- Promptly notify the DSS (PIC) or OPM (FIPC) if the investigation is no longer needed; and
- Limit access through strict need-to-know, thereby requiring fewer investigations.

Close observance of the above guidelines will allow the DSS and the OPM to operate more efficiently and permit more effective, timely, and responsive service in accomplishing investigations. It will also allow you to perform your job more effectively and efficiently by reducing the number of PSIs for you to adjudicate.

DETERMINING POSITION FUNCTIONS

All commanders of employing activities and heads of DoD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of the regulation.

The issuance of a personnel security clearance eligibility by the CAF is a function distinct from that involving the granting of access by the employing activity to classified information. The CAF also determines if an individual is eligible for access to SAP information, or is suitable for assignment to sensitive duties or other duties that require a trustworthiness determination.

"Clearance eligibility determinations are made on the merits of the individual case."

Clearance eligibility determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance eligibility. Access determinations by the employing activity are made solely on the basis of the individual's need-to-know in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for

cause without applying the provisions of DoD 5200.2R, paragraph 8-201.

Access to classified information is made by the employing activity.

Access to classified information is granted to persons whose official duties require it and who have the appropriate personnel security clearance. Access Determinations (other than for Special Access Programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander of an employing activity that access is officially required.

It is very important that you understand the provision of E.O. 12356 part 4 which places strict limitations on the dissemination of official information and material.

In the absence of derogatory information, DoD commanders and organizational managers must accept a personnel security clearance determination, issued by any authorized DoD authority, as the basis for granting access without requesting additional investigation or investigative files.

RESPONSIBILITY FOR ACCESS SUSPENSION

Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to an individual's ability or intent to protect classified information. Upon receipt of the initial derogatory information, it is the commander's or employing activity's responsibility to determine what action to take, based on all available information.

The employer has the option, at this point, to either continue the subject's access status unchanged (because it is in the interests of national security), or take the necessary action to suspend access until a final determination is made by the CAF regarding the

When access is no longer required it is administratively downgraded or withdrawn.

subject's clearance status. When regular access to a prescribed level of classified information is no longer required in the normal course of an individual's duties, eligibility level is administratively downgraded or withdrawn, as appropriate.

For you to effectively do your assigned job as an adjudicator, you must know when a clearance is valid, and when it is not. Figure 2-2 will help you to make this determination and to see how long a personnel security clearance remains valid.



A personnel security clearance remains valid until:

1. The individual is separated from the Armed Forces,
2. The individual is separated from DoD civilian employment,
3. The individual has no further official relationship with DoD,
4. Official action has been taken to deny, revoke or suspend the clearance or access, or
5. Regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties.

If an individual resumes the original status of (1),(2),(3) or (5) above, no single break in the individual's relationship with DoD exists greater than 24 months, and the need for regular access to classified information at or below the previous level recurs, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

Figure 2-2

REMINDER

A Personnel Security Clearance is an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the security clearance being granted. Although being granted a security clearance is a privilege, an organization may suspend access for cause when serious questions regarding trustworthiness arise. When regular access to a prescribed level of classified information is no longer required, it must be administratively downgraded or withdrawn, as appropriate. Employing activities ensure that clearance applications are submitted only when

necessary, that they are accurate and complete, and that security clearance records are properly maintained.

REQUESTING PERSONNEL SECURITY INVESTIGATIONS

Now we will introduce you to the requesting procedures for Personnel Security Investigations (PSIs) and identify those who are authorized to originate the request for investigation. You will also learn what authorities are responsible for determining if individuals under their jurisdiction require a PSI, and the type that will be required, depending on position sensitivity.

DETERMINATION AUTHORITIES

Earlier you learned about the responsibilities of the employing activities for requesting PSIs on DoD affiliated personnel. You know the requests for PSIs will be limited to those required to accomplish the DoD mission. Who else can request PSIs? Do the requesters have to be authorized? These are valid questions that must be answered. The answers can be found in Fig.2-3 which identifies other authorized requesters. Only those designated are authorized to submit requests for Personnel Security Investigations.

AUTHORIZED REQUESTERS

DoD 5200.2R

A. Military Departments

- (1) Army
 - (a) Central Clearance Facility
 - (b) All activity commanders
 - (c) Chiefs of recruiting stations

- (2) Navy (including Marine Corps)
 - (a) Central Adjudicative Facility
 - (b) Commanders and commanding officers of organizations listed on the Standard Navy Distribution List
 - (c) Chiefs of recruiting stations

- (3) Air Force
 - (a) Central Adjudication Facility
 - (b) Assistant Chief of Staff for Intelligence
 - (c) All activity commanders
 - (d) Chiefs of recruiting stations

B. Defense Agencies -- Directors of Security and activity commanders.

C. Organization of the Joint Chiefs of Staff--Chief, Security Division.

D. Office of the Secretary of Defense--Director for Personnel and Security, Washington Headquarters Services.

E. Commanders of Unified and Specified Commands or their designees.

F. Such other requesters approved by the Deputy Under Secretary of Defense for Policy.

Figure 2-3

You will notice in Figure 2-3 that one of the authorized requesters is the CAF for each Military Department.

CAF makes determination for eligibility.

Why would a CAF request PSIs? You adjudicate PSIs which others have requested, right? You make the decision or determination for eligibility based on the merits of the case. In order for you to make a common sense decision, you will often have to reopen or ask DSS or OPM for an SII on the case you are adjudicating. Therefore, it shouldn't surprise you to

learn that the CAF is a major requester of PSIs.

We will show you that the SII is one of the PSIs authorized in the DoD PSP. Whenever you request an SII from DSS or OPM, or ask to reopen an SSBI for additional work, you are in effect requesting a PSI.

As you can see, the employing activity is only one of the authorized requesters of PSIs within the DoD. The designated authorities in Fig.2-3 will be held responsible for determining if individuals under their jurisdiction require a PSI, per DoD 5200.2R.

In order for the process to work effectively, there must be proper planning (by the requesting activity) to ensure investigative requests are submitted sufficiently in advance to allow completion of the investigation before it is needed to grant the required clearance eligibility or otherwise make the necessary personnel security determination.

CRITERIA FOR REQUESTING INVESTIGATIONS

The authorized requesters listed in Fig.2-3 have specific guidelines to follow when requesting an investigation.

First determine the type of investigation to be requested

First they must determine the type of investigation to be requested to meet (but not exceed) the investigative requirements for the specific position or duty assignment.

DoD uses seven types of PSIs for the Personnel Security Program (PSP):

The NACLC, ANACI and SSBI are used primarily for initial assignment to duties.

The PR, SPR CPR and SII are used as part of the Continuous Evaluation Program (CEP).

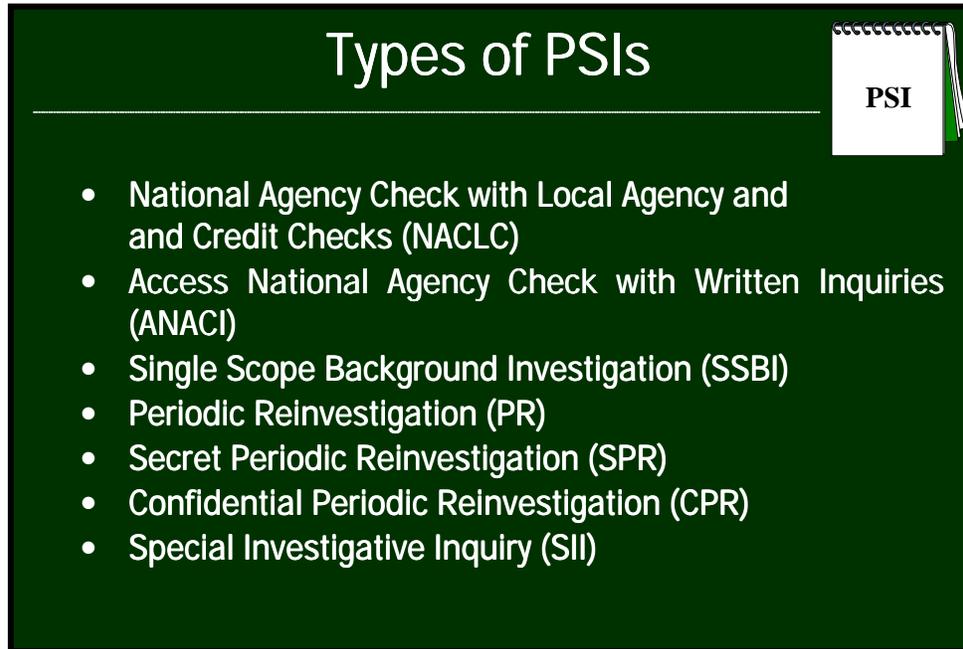


Figure 2-4

In addition, the activity has to decide if any special requirements exist because of the individual's status (citizenship, job description, etc), and the duty (position) requirements. An example of this would be an individual who is a U.S. national civilian employee whose duties require him/her to be assigned to a Critical sensitive position.

The activity must initiate the corresponding documents for an SSBI before the individual can be assigned to the position. DoD 5200.2R, Appendix D and the 22 Aug 00 memo contain processing instructions and tables for requesting investigations as a guide for requesters. The activity must then prepare and forward the requests for PSIs to the appropriate investigative agency (DSS or OPM) to ensure efficient and effective completion of the investigation in a timely manner.

PSI REQUEST PACKAGES

Each PSI has its own request forms.

Just as each type of PSI has different uses and scope, so each uses different request forms. It is important for you to be familiar with each form used and with the investigation with which it is used. As you will discover, these forms provide information which is as critical to the adjudicative process as to the investigative process.

You should familiarize yourself with them so that you can make the best possible use of them when reviewing and adjudicating an investigation.

Figure 2-5 will give you a basic understanding of the forms we will be using in the Personnel Security Program.

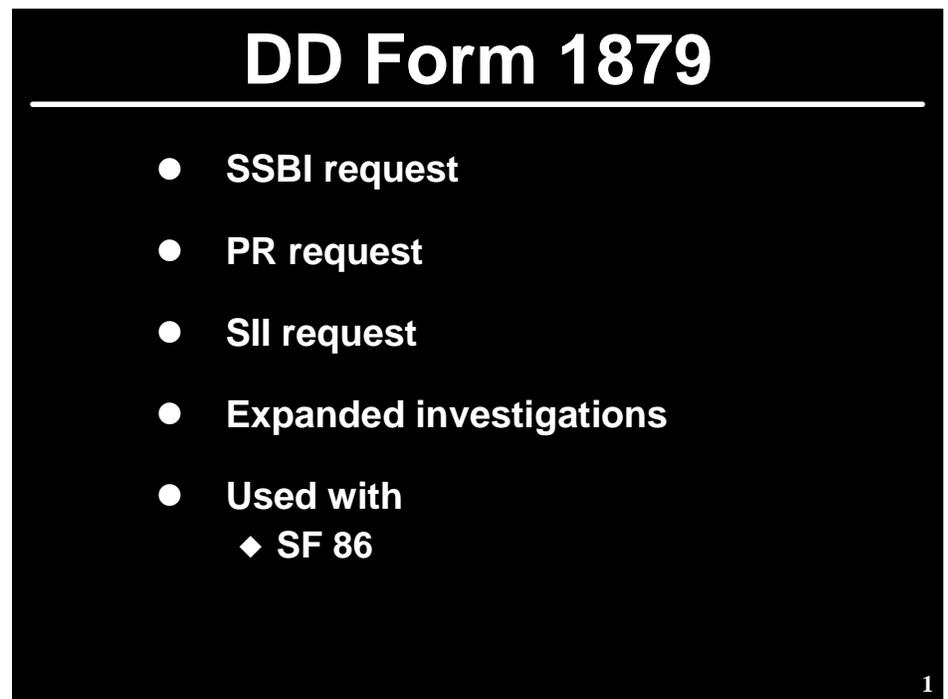


Figure 2-5

Effective 1 January 1996, the Standard Form 86 is the only form used for access to classified information. The SF 86 may be used with any Personnel Security Investigations that requires access.

Standard Form 86

- 86 used for all classified access
- All military investigations
- Can be used in all PSIs
- Seven year coverage in some questions
- No time periods in other questions

11

Figure 2-6

The SF 85P is used for positions of public trust and other positions that **do not** require access to classified information.

Standard Form 85P

- SF 85P used for
 - ◆ Public trust positions w/o access
 - ◆ Other duties not requiring access
- Seven year coverage in some questions
- One year on personal drug use
- Other items do not have time limits

12

Figure 2-7

The SF 85PS is used in conjunction with the SF 85P for positions designated by the base. The base must obtain prior approval from the Office of Personnel Management to use the SF 85PS.

The SF 85PS has three questions to supplement the information contained in the SF 85P. They concern **mental health** treatment, **alcohol** use and **drug** involvement.

One question on the form asks if there has been any use of drugs while employed as a law enforcement officer, prosecutor, courtroom official, while possessing a security clearance or while employed in a public safety position.

Standard Form 85 PS

- Used with SF 85P for designated positions
- Must have OPM approval to use
- Has three questions
 - ◆ Mental health
 - ◆ Alcohol involvement
 - ◆ Drug involvement

13

Figure 2-8

DoD uses two different types of fingerprint cards as shown Figure 2-9. The only differences are in the information provided on the top half of the cards.

Fingerprint Cards FD 258 and SF 87

- **FD 258 is used for**
 - ◆ **SSBI**
 - ◆ **PR**
 - ◆ **Secret PR**
 - ◆ **NAC**
 - ◆ **SII (if required)**
- **SF 87 is used for NACI or ANACI only**



14

Figure 2-9

DoD uses two primary investigative agencies to conduct PSIs. These are the Defense Security Service (DSS) and the Office of Personnel Management (OPM). DSS conducts all investigations on military personnel cept the NACLCS and accessions for the Air Force, Navy and Marines which are conducted by OPM. DSS also conducts investigations on all contract personnel and NAF Positions of Trust. OPM conducts all investigations for civilian employees.

Investigative Agencies

| | <i>DSS</i> | <i>OPM</i> |
|---|---|---|
|  | SSBI TS-PR Accessions for Army & Coast Guard | NACLC Accessions for Air Force, Navy & Marines |
|  | NAF Position of Trust | ANACI SSBI All PRs |
|  | All | |

Figure 2-10

Now let's take a closer look at the different investigations used in the DoD. The Electronic Personnel Security Questionnaire (EPSQ) can be forwarded to DSS (electronically transmitted only) and OPM (must be printed hard copy vices electronic submission).

ENTNAC/NACLC/ACCESSIONS/S-PR/C-PR

For guidance on submission of these investigations, please refer to the August 22, 2000 memorandum, "Personnel Security Investigations".

NACI/ANACI (National Agency Check with Written Inquiries & Access National Agency Check with Written Inquiries)

When a **NACI** is requested for a civilian in a **NON-SENSITIVE** position, the forms shown in Figure 2-11 must be sent to **OPM**

SF 85 (Questionnaire for Non-Sensitive Positions)

**Any official application for Federal Employment (SF-171;
OF-612; Resume)**

SF 87 (CSC Fingerprint Card)

Figure 2-11

Figure 2-12 shows the forms sent to OPM when a
ANACI is requested for a civilian in a **NON-CRITICAL
SENSITIVE** position.

SF 86 (Questionnaire for National Security Positions)

**Any official application for Federal Employment (SF-171;
OF-612; Resume)**

SF 87 (CSC Fingerprint Card)

Figure 2-12

Figure 2-13 shows the forms sent to OPM when a NACI is
requested for employment in a **Public Trust** position.

SF 85P (Questionnaire for Public Trust Positions)

**Any official application for Federal Employment (SF-171;
OF-612; Resume)**

SF 87 (CSC Fingerprint Card)

Figure 2-13

SSBI and SSBI-PR

When requesting an **SSBI** or **SSBI-PR** from DSS, the requester must submit the forms shown in Figure 2-14 when the subject is a **military member or civilian employee**.

DD Form 1879 (Request for PSI)

SF 86 (Electronic Personnel Security Questionnaire)

FD 258 (Fingerprint Card)

Figure 2-14

Figure 2-15 shows the forms sent to **DISCO** for **Defense Contractor**.

DD Form 1879 (Request for PSI)

SF 86 (Electronic Personnel Security Questionnaire)

FD 258 (Fingerprint Card)

Figure 2-15

Special Investigative Inquiry (SII)

This investigation is a vital part of the Continuous Evaluation Program (CEP). This investigation is unique. All other DoD investigations have standard coverage requirements - like 7 or 10 years, neighborhood coverage, employment coverage, etc. upon which a clearance eligibility can be granted.

The SII has no standard coverage and for that reason a clearance eligibility can never be granted using an SII for its basis.

The SII is requested and intended to prove or disprove security concern issues and could be the basis for denial or revocation of a security clearance.

When requesting an SII from DSS, the forms shown in Figure 2-16 must be used:

DD Form 1879 (Request for PSI)

SF 86 (Electronic Personnel Security Questionnaire)

***FD 258 (Fingerprint Card)**

If pertinent, the results of a recently completed NAC, NACLC, ANACI or other related investigative reports or documents should also accompany the request.

(* If these documents have been submitted to DSS as part of a PSI in the last 12 months, they do not need to be re-submitted.)

Figure 2-16

PRIORITY REQUESTS

You may also have heard about "**Priority Requests**" for investigations. These requests for priority (hurry-up) for individual investigations or categories of investigations should be kept to a minimum.

As a matter of fact, DSS will not assign priority to any PSI or categories of investigation without written approval of the Deputy Under Secretary of Defense for Policy. Given that bit of information, it is unlikely that an activity will initiate this type of investigation or ask you or your CAF to get DSS to give a PSI priority handling.

REMINDER

The requesters of Personnel Security Investigations must be authorized and designated IAW existing regulations.

They must be able to identify the type of investigation necessary to accomplish the activity mission, and to ensure the individuals under their jurisdiction need the investigation.

The request for PSI must be submitted IAW guidelines to ensure they are complete and accurate, which will in turn get a timely response from the investigative agency.

INTERIM CLEARANCE ELIGIBILITY PROCESS

"Who is authorized to grant an interim clearance?"

Here you will learn the process for determining interim clearance eligibility.

What is the criteria for interim clearances?

What kind of restrictions apply? Who is authorized to grant an interim clearance? What are the investigative requirements for Interim Top Secret, Interim Secret and Interim Confidential clearances, and what individuals are eligible for each?

We will also look at two other methods of giving individuals access to sensitive information. They are known as one-time access and emergency appointments.

You will also see what kind of relationship they have to the interim type clearances.

When we are finished here you should be able to answer the following questions:

- * What is an "Interim Clearance?"
- * Who can grant an interim clearance?
- * What restrictions apply to interim clearances?
- * What are the steps in determining eligibility for an interim clearance?
- * What is the difference between one-time access and interim clearance?
- * What is an emergency appointment?

INTERIM SECURITY CLEARANCES

Interim security clearances may be granted to DoD military, civilian and contractor personnel.

For you to do your job as an adjudicator, you need to know a lot of things, as you are finding out. One of these is to know what an interim security clearance is and when it can be granted. DoD military, civilian and contractor personnel who are employed by or serving in a consultant capacity to the DoD, may be considered for access to classified information only when such access is required in connection with their official duties.

These individuals may be granted either a final or interim personnel security clearance provided the investigative requirements in the regulation are complied with and all

available information has been reviewed and a determination made that such a clearance would be clearly consistent with the interests of national security.

The interim clearance is a security clearance based on the completion of certain minimum investigative requirements, and which is granted on a temporary basis, pending the completion of the full investigative requirements.

GRANTING AUTHORITIES

An employing DoD component may issue an interim clearance eligibility to individuals under their administrative control pending a final eligibility determination by the individual's own component. When this situation occurs, the issuing component must provide written notice of the action to the parent activity.

There are only certain officials who are authorized to grant, deny or revoke personnel security clearances (Top Secret, Secret and Confidential). This includes interim clearances. Figure 2-17 lists those authorities that can grant interim clearances, which include the activity level where authorized or designated by proper authority.

INTERIM GRANTING AUTHORITIES

- Secretary of Defense and/or designee
- Secretary of the Army and/or designee
- Secretary of the Navy and/or designee
- Secretary of the Air Force and/or designee
- Chairman, Joint Chiefs of Staff and/or designee
- Directors of the Defense Agencies and/or designee
- Commanders of the Unified and Specified Commands and/or designee

Figure 2-17

INVESTIGATIVE REQUIREMENTS

As in everything we do as adjudicators, there are requirements and restrictions. Dealing with interim clearances is no exception, and because of their nature, they probably have more variations of use than any other type of security clearance. Figures 2-18 and 2-19 identifies the investigative requirements for interim clearances.

Interim Top Secret Clearance (*Civilian or Military*)

Available Top Secret billet (if used)

Favorable local records check of Personnel Files, Base military/security police files, Medical records and other base files.

Favorable review of SSBI request package

SSBI requested

NAC portion favorably completed OR an existing, favorable NAC, NACL, ENTNAC, NACI or ANACI

17

Figure 2-18

Interim Secret/Confidential Clearance (Civilian/Military Employees)

Favorable local records check

- Personnel files
- Base military/security police files
- Medical records
- Other base files

Favorable review of PSI request package

**NACLC for military members or
ANACI for civilian employees requested.**

14

Figure 2-19

INTERIM CLEARANCE RESTRICTIONS

As we already know, personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements. The restrictions that apply to final clearances also apply to interim clearances. Figure 2-20 and 2-21 shows instances where interim personnel security clearances will not be issued. Some of the positions, however, may involve sensitive duties and require an investigation and adjudication as such. If activities follow these restrictions, unnecessary PSIs will not be initiated and the adjudicator will have less to consider when reviewing PSIs.

Restriction on Clearances

Security clearances will not be issued to certain persons, for example:

- > Non-U.S. Citizens**
- > Civilians in nonsensitive positions**
- > Persons with inadvertent access**

See Figure 2-24 for a complete listing.

12

Figure 2-20

INTERIM CLEARANCES NOT ISSUED:

- ◆ To persons in nonsensitive positions.
- ◆ To persons whose regular duties do not require authorized access to classified information.
- ◆ For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.
- ◆ To persons who may only have inadvertent access to sensitive information areas, such as guards, emergency service personnel, firemen, doctors, nurses, police, ambulance drivers, or similar personnel.
- ◆ To persons working in shipyards whose duties do not require access to classified information.
- ◆ To persons who can be prevented from accessing classified information by being escorted by cleared personnel.
- ◆ To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.
- ◆ To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.
- ◆ To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.
- ◆ To perimeter security personnel who have no access to classified information.
- ◆ To drivers, chauffeurs and food service personnel.

Figure 2-21

ONE-TIME ACCESS

We will now show you the close relationship between Interim clearances and One-Time Access. Sometime during your career, you may encounter circumstances that arise where an urgent operational or contractual emergency exists for cleared DoD personnel to have short duration access to classified information at a higher level than is authorized by their existing security clearance eligibility. This happens most often when someone has a Secret clearance and needs access to Top Secret information for a short period of time. Since the access will be short-term, is it worth the time and expense of conducting another Personnel Security Investigations?

One-Time Access Requirements

- Usually happens when one-time TOP SECRET access is needed
- If one-time or very short period, it isn't worth an SSBI
- Use up to 90 days



Figure 2-22

Close relationship between interim clearances and one-time access.

You will find that in many instances, the processing time required to upgrade the clearance would not permit timely access to the information in question. In this type of situation (and only for compelling reasons to ensure the success of the DoD mission), an authority referred to in DoD 5200.2R, para 3-407a, is authorized to grant higher level access on a temporary basis, subject to the terms and conditions listed.

There are several administrative requirements for using the one-time access procedures as shown below.

One-Time Access Requirements

- **Approval by**
 - ◆ General/Flag Officer
 - ◆ GCM authority
 - ◆ SES equivalent
- **Must be US citizen**
- **Must have current DoD clearance**
- **Access at one higher level**



38

Figure 2-23

The access must be at the next higher level. In the situation where someone currently has a Confidential clearance and needs Secret access, these procedures do not apply. The reason for this is the PSI used for Confidential clearances is also used for Secret clearances.

One-Time Access Requirements

- **Has been employed for at least the last two years**
 - ◆ **Military**
 - ◆ **Civilian**
 - ◆ **Contractor**
- **Full-time personnel only**
- **Favorable local records check**
- **Access limited to one or just a few times**



39

Figure 2-24

The security determination made by a CAF is for Secret *eligibility*, even if a Confidential clearance is requested. So, if the person has a Confidential clearance, they already have the PSI for a Secret clearance.

The person must have been employed in a military, civilian, or contractor capacity for the last two continuous years. If the person has had a break in service, employment, or contract status within the last two years, then these procedures cannot be used.

The procedures apply to full-time personnel only. They do not apply to part-time civilian employees or reserve military personnel in an inactive status.

The base or installation must conduct a local records check. If the checks turn up potentially derogatory information, then the one-time access cannot be used. That information should be reported to the CAF. The records checks include:

- **Personnel**
- **Security/law enforcement/intelligence**
- **Medical**
- **Special programs**
- **Other locally available records**

The access must be limited to one or just a few times. If the person will require access on a recurring basis, process him or her for the higher level clearance.

This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for a higher level clearance.

As you can see, the interim clearances and one-time access are designed for a short period of time depending on the circumstance. The object is to get an individual (who meets the requirements) quick access because of circumstances that arise. Both of these meet the criteria of that mission and are in accordance with DoD policy.

Although the very purpose is different, the main difference between interim clearances and one-time access is the length of time they are valid for. An interim clearance eligibility is valid until the completion of the investigation and may be terminated sooner if unfavorable information is developed that would warrant rescinding the interim eligibility.

EMERGENCY APPOINTMENTS

We have looked at several ways an individual can get a security clearance. The one way we will now discuss is known as **Emergency Appointments**. The emergency appointment is strictly a personnel action by the Civilian Personnel Office (CPO) or head of the requesting organization or activity. They have several options for this appointment as shown below.

Emergency Appointment to a Civilian Position (Civilian Personnel Requirements)

Options for a new civilian employee

- ◆ Wait until PSI completed and then the CPO makes the final appointment
- ◆ CPO makes an emergency appointment pending completion of the PSI, but no interim clearance is granted by the Security Office
- ◆ CPO makes emergency appointment and the Security Office grants the interim clearance
- ◆ Only the CPO can appoint to a Federal position



Figure 2-25

This applies to civilian employees in Noncritical sensitive and Critical sensitive positions. In both cases an emergency situation must exist, whereby the delay in appointing the individual would be considered harmful to the national security as determined by the employing activity. An ANACI must have been submitted for the Noncritical sensitive position before the position can be filled.

When this has been accomplished, an interim clearance may be issued (but is not required by regulation to be requested or granted) provided all the requirements of an interim clearance (as explained earlier in this lesson) have been met.

For the Critical sensitive position an SSBI must be submitted.

However, the position may only be filled when the NAC portion of the SSBI or a previous valid NAC, ANACI, NACL or ENTNAC has been completed and favorably adjudicated. The emergency appointment is strictly a personnel action by the head of the requesting organization or activity.

SPECIAL ACCESS PROGRAMS

Here you will learn about Special Access Programs within the DoD; how they are structured and mandated; why the programs were designed, and what DoD regulation governs them.

We will discuss the various investigative requirements for each program, who they pertain to, and the criteria that must be met before access can be granted.

READING ASSIGNMENT

DoD 5200 2R Chapter 1: para. 1-324

DoD 5200 2R Chapter 3: Sections 3 & 5

DoD 5200 2R Chapter 7: all

DCID 6/4: all

WHAT ARE SPECIAL ACCESS PROGRAMS ?

A Special Access Program (SAP) is any program that is designed to control access, distribution and protection of particularly sensitive information. SAPs have investigative and other requirements over and above those for a personnel security determination.

Special Access Programs

DoD Directive O-5205.7

Secret clearance minimum

SAP PSM makes final decision

**Most SAPs upgraded to
SSBI and PR requirements**

46

Figure 2-26

Special Access Programs (SAP) created under authority of DoD O-5205.7 require a final Secret clearance as the minimum.

The SAP Program Security Manager makes a final eligibility determination for entry/retention in the SAP. This decision is separate from the security clearance decision. Possession of the security clearance does not automatically mean the person will be approved for SAP access.

Most SAPs require the SSBI and PR due to their extreme sensitivity.

All SAPs are considered sensitive duties, requiring both a personnel security determination and another determination for entry/retention in the SAP by a designated official. A SAP may be considered a formalized "need-to-know" system with additional requirements for access, dissemination and storage of information. These additional requirements and controls are necessary due to the very sensitive nature of the information or duties.

Entry into a SAP requires that the individual be nominated for a position that requires access to the protected information or performs duties necessary to carry out the mission of the SAP. In addition to the investigative requirements shown below, additional requirements for entry/retention in the SAP may be established to ensure that only qualified personnel are initially assigned or retained in the SAP.

SAPs are established with the approval of senior Executive Branch officials. DOD 5200.1R, Department of Defense Information Security Program Regulation, governs the establishment of SAPs within DOD. Section Five, Chapter Three of the DOD 5200.2R, prescribes the investigative requirements for the SAPs. Directives governing each SAP will include necessary investigations, special requirements and administrative procedures for the SAP.

The investigative and adjudicative requirements of the regulation cover only the personnel security determination portions for these programs. The additional determinations made by SAP officials are separate decisions made to permit entry/retention into the SAPs. For example, an individual who is nominated for assignment to Category I Presidential Support duties and requires a TOP SECRET security clearance would receive two determinations. First, a personnel security determination would be made on the TOP SECRET clearance by a CAF. The second determination would be for assignment to Presidential Support duties and would be made by an authorized official for the SAP.

SAPs and Their Investigative Requirements

The following is a list of the SAPs and their investigative requirements:

| <u>SAP</u> | <u>PSI Required</u> |
|--|---------------------|
| ◆ Sensitive Compartmented Information (SCI) ¹ (This program involves access to information/sources/methods about intelligence operations of the United States) | SSBI & SSBI-PR |
| ◆ Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) (This program involves access to information about the military plans of the United States) | SSBI |
| ◆ Presidential Support Activities-Category I ² (This program involves certain duties supporting the Commander-in-Chief) | SSBI & SSBI-PR |
| ◆ Presidential Support Activities-Category II ^{2,3} (This program involves certain duties supporting the Commander-in-Chief) | SSBI & SSBI-PR |
| ◆ Nuclear Weapon Personnel Reliability Program (PRP) Critical Position ¹ (This program involves access to certain nuclear information/ materials/weapons) | SSBI |

| | |
|---|---------------------------|
| <ul style="list-style-type: none"> ◆ Nuclear Weapon PRP Controlled Position¹ (This program involves access | <p>NACLCL or ANACI</p> |
| <p>to certain nuclear information/ materials/weapons)</p> | |
| <ul style="list-style-type: none"> ◆ Access to North Atlantic Treaty Organization (NATO) Classified Information COSMIC (TOP SECRET)¹ (This program involves staff positions within the NATO command structure) | <p>SSBI & SSBI-PR</p> |
| <ul style="list-style-type: none"> ◆ Access to NATO SECRET^{1,4} (This program involves staff positions within the NATO command structure) | <p>NACLCL or ANACI</p> |
| <ul style="list-style-type: none"> ◆ Access to NATO CONFIDENTIAL¹ (This program involves staff positions within the NATO command structure) | <p>ANACI or NACLCL</p> |
| <p>FOOTNOTES: 1 - PSI must have been completed within last five years 2 - PSI must have been completed within last twelve months 3 - Same NAC on spouse/family members as SSBI 4 - A new NACLCL is required every five years</p> | |

Figure 2-27

SUMMARY

SAPs are established to control access, distribution and protection of particularly sensitive information. DOD 5200.1R governs the establishment of SAPs within DOD. Each SAP is governed by a separate directive; however, the investigative requirements are contained in the DoD 5200.2R. A subject needing access to information in a SAP to perform the position duties will be nominated for the SAP and investigated.

Review Exercise

1. **What are the three levels of position sensitivity used in DoD?**

2. **The highest sensitivity level used in DoD for civilian sensitive positions is _____.**

3. **An SSBI is the minimum investigation to support assignment to _____.**

4. **Which of the following establishes levels of position sensitivity used in the DoD Personnel Security Program?**

- a. DoD 5200.27
- b. DoD 5200.1R
- c. DoD 5200.2R
- d. None of the above

5. **Security clearance determinations are made on the merits of the individual case.**

- a. True
- b. False

- 6. The investigative request process should limit access through strict _____ - _____ - _____, thereby requiring fewer investigations.**
- 7. A list of authorized requesters for PSIs can be found in which of the following documents?**
- a. DoD 5200.2-R
 - b. E.O. 10450
 - c. Privacy Act of 1974
 - d. Public Law 81-733
- 8. Military department activity commanders are authorized to request PSI's.**
- a. True
 - b. False
- 9. What type investigation would a U.S. national military member need if the duties required access to SIOP-ESI?**
- _____
- 10. A U.S. national military member whose duties require a Secret clearance would be the subject of a ANACI investigation.**
- a. True
 - b. False
- 11. Within the DoD, who may be granted an interim clearance?**
- _____
- _____

- 12. An interim Top Secret clearance eligibility for a DoD civilian member can be granted provided the _____ has been favorably completed or an favorable _____ exist.**
- 13. An individual must have been continuously employed by a DoD component for the preceding _____ months to be afforded one-time access to a higher level access.**
- 14. Within the DoD it is necessary to restrict personnel security clearances to the absolute minimum to meet mission requirements.**
- a. True
 - b. False
- 15. Which of the following may not be granted an interim clearance without further justification?**
- a. Persons in non-sensitive positions
 - b. Drivers
 - c. Chauffeurs
 - d. All of the above
- 16. For how long are one-time access authorizations normally valid?**
-

17. SAP's normally exceed established investigative requirements, thereby are authorized only when mandated by _____, _____ or _____.

18. Personnel assigned to honor guards, ceremonial units and military bands who perform at Presidential functions and facilities would be in which of the following Presidential Support categories?

- a. 1
- b. 2
- c. 3
- c. 4

19. Personnel nominated for category one duties must have been the subject of what type investigation in addition to other investigative requirements?

20. What DoD regulation governs establishment of SAPs in DoD?

Solutions & References

1. **Critical-Sensitive
Noncritical-Sensitive
Non-Sensitive** (Lesson 2, page 2-5)
2. **Critical-Sensitive** (DoD 5200.2-R, para 3-101;
Lesson 2, page 2-5)
3. **Critical-sensitive duties.** (Lesson 2, page 2-6)
4. c. **DoD 5200.2R** (Lesson 2, page 2-7)
5. a. **True** (Lesson 2, page 2-11)
6. **need-to-know** (Lesson 2, page 2-10)
7. a. **DoD 5200.2-R** (Chapter V; Lesson 2, page 2-16)
8. a. **True** (Lesson 2, page 2-15)
9. **SSBI** (Lesson 2, page 2-40; DoD 5200.2-R, Appendix D)
10. b. **False** (Lesson 2, page 2-6, DoD 5200.2-R,
Appendix D)
11. **Military, civilian and contractor personnel who are
employed by DoD or serving in a consultant capacity to
DoD.**
(Lesson 2, page 2-27).

12. **NAC portion, investigation** (Lesson 2, page 2)
13. **24 months** (DoD 5200.2-R, para 3-407;
Lesson 2, page 2-34)
14. a. **True** (Lesson 2, page 2-32)
15. d. **All of the above** (Lesson 2, page 2-31)
16. **90 days** (Lesson 2, page 2-32)
17. **statute, national regulation, or international agreement,
or EO 12968 or its successor.** (DoD 5200.2-R, para 3-500)
18. b. 2. (DoD 5200.2-R, para 3-503)
19. **SSBI & SSBI-PR** (Lesson 2, page 2-40)
20. **DoD 5200.1-R** (Chapter III, Section 5,
Lesson 2, page 2-41)