



**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

❖ NOTICE ❖

We have made every effort to ensure that the content of this independent study course accords with all applicable policies in effect at the time it was printed. However, such policies may change in the interval between printings, and the technical accuracy of a given edition of the course cannot be guaranteed in all particulars. Questions regarding the technical accuracy should be directed to your Central Adjudication Facility or Security Officer. However, you should base your responses to the questions in the course examinations solely on the information provided in the course material and not on any other source.

(Note: DoD policy guidance concerning the security clearance restrictions mandated by the 2001 Defense Authorization (Title 10 U.S.C.986) U.S.C.986) was pending final implementation as of the December 2000 revision of this course material. Future course updates will include the particulars of this policy change.)

Revised: December 2000

Contents

	Page
GENERAL INFORMATION AND CONTENTS	1-6
Course Objective	6-7
Acronyms and Abbreviations	8-11
Introduction	12
LESSON 1	
Overview of the Personnel Security Program	1-1/1-48
LESSON 2	
Employing Activities' Initial Responsibilities	2-1/2-49
LESSON 3	
Personnel Security Investigations	3-1/3-77
LESSON 4	
Central Adjudication	4-1/4-43
LESSON 5	
Adjudicative Issues	5-1/5-79
LESSON 6	
Continuous Evaluation	6-1/6-24

Reading Assignments

- DoD 5200.2R (January 1987 - Change 1, 2, &3)
- 10 November 1998 Memorandum - Personnel Security Investigations and Adjudications
- DCID 6/4 (July 1998)
- Recent Espionage Cases (July 1997)
- 22 August 2000 Memorandum – Personnel Security Clearance Investigations

General Information



HISTORY

The Department of Defense Security Institute (DoDSI) created the DoD Personnel Security Adjudications Course (PSAC) in response to the August 1986 recommendations of the Defense Security Review Commission (commonly referred to as the Stillwell Commission). DoDSI developed the course in coordination with the Office of the Director, Counterintelligence and Investigative Programs, Office of the Secretary of Defense (OSD) which has responsibility for the DoD Personnel Security Program; the Office of the General Counsel, OSD; the major DoD Component Central Adjudication Facilities (CAF); and the Defense Personnel Security Education and Research Center. The course was to consist of two phases: a prerequisite independent study course followed by a resident training course.

In 1998, the responsibility for managing and conducting the adjudication training was transferred to the Defense Security Service Academy (DSSA).

PURPOSE

This independent study course is designed to provide basic knowledge of the DoD Personnel Security Program's major features and an introduction to several key areas presented in the resident course. Students nominated to attend the resident course must first successfully complete this course.

The resident course instruction will address some of the independent study course material in greater depth, and will include elements of the independent study course in the resident Practical Exercises (PE's)

ADMINISTRATION

This independent study course is administered through ENROL. When a student registers they can begin training immediately. The course materials are available online, downloadable, or by request on CD-Rom through the course website.

When the student is ready to take the exam they may go online and take the final examination. The test is scored automatically. The student will know if they passed or failed immediately. Within 48 hours, a successful grade will be entered into ENROL and the course will be closed.

A passing grade is **76%** or greater.

STUDYING THE LESSONS

Complete the independent study course in the sequence written. To get the most out of each lesson, follow this procedure:

Note the lesson objectives and refer to them from time to time as you go through the lesson text.

If there are reading assignments complete them for each lesson **prior** to beginning your study of the lesson.

Complete the review exercises for each lesson. Refer to the lesson text to check your answers. If you answer a lesson exercise incorrectly, review the lesson material again to be sure you know and understand the correct response.

Lesson exercises are for your review and practice only. Do not turn them in for grading.

CONTENT ASSISTANCE

If you have a question about the content of this course, contact the DSSA Personnel Security Team Course Administrator for assistance.



To phone us, use one of these numbers:

◆ DSN: 283-8189/8191 COM: (410) 865-3189/3191

◆ To write to DSSA:

Defense Security Service Academy (DSSA)
ATTN: Personnel Security Team
938 Elkridge Landing Rd
Linthicum, MD 21090

TIME LIMIT

You are allowed up to one year from date of enrollment to satisfactorily complete this independent study course. Extensions may be granted upon receipt of a written request justifying the extension.

You must successfully complete the current final examination within 90 days of your attendance at the resident course. If circumstances prevent your attendance and you have successfully completed the final examination, you must retake and pass the current final examination under the same time conditions before DSSA will allow you to attend the resident course.

LESSON AND END OF COURSE EXAMINATIONS

When you have completed all six lessons and believe you can meet their objectives, do the following:

- The final examination is online at the course web site. It will have appropriate instructions for its completion.
- When you have completed the final examination, the system will grade the exam and let you know if you passed.

You may not retain or copy your answer sheets or the examinations.

The passing score for the final examination is 76% (for example, at least 38 items correct out of 50).
If you score less than 76%, you must retake and successfully complete the full examination.

CREDIT

The American Council on Education (ACE) assessed this course for college credit hour equivalents, and made the following credit recommendations:

**DoD Personnel Security Adjudications
(Independent Study Course)**

In the vocational certificate category, three semester hours in Personnel Security Adjudications.

**DoD Personnel Security Adjudications Course
(Resident Phase)**

In the lower division baccalaureate/associate degree category, three semester hours in Personnel Security Adjudications.

DSSA CERTIFICATE

When you have successfully completed the exam for this independent study course, an online Certificate of Accomplishment will be available for printing.

COURSE OBJECTIVES

When you have completed this course, you should be able to do the following:

- State the purpose of the DoD Personnel Security Program (PSP) and describe the roles of civilian, military and contractors within the PSP.
- Explain the major elements of the PSP.
- Explain what a Personnel Security Clearance (PCL) is, its purpose, and the conditions on which it is based.
- Explain the different types of threats to the national security and how to identify potential vulnerabilities.
- State the regulation that applies to civilian position sensitivity designations and who can designate each level.
- State the criteria for requesting personnel security investigations and identify those authorized to originate the request.
- State which investigative agencies are authorized to conduct Personnel Security Investigations for DoD and under what authority.
- Differentiate various types of investigative forms used in each type of personnel security investigation.

Explain the thirteen guidelines and describe the procedures used in determining eligibility for access to classified information and/or assignment to a sensitive position.

COMMON ABBREVIATIONS AND ACRONYMS

As you take this course, you'll see a lot of abbreviations and acronyms which are part of the adjudicator's jargon. Below is a listing of the most common, along with their meanings.

<u>Acronym</u>	<u>Meaning</u>
ADR	Adjudicative Desk Reference
AFCAF	Air Force Central Adjudication Facility – the CAF for the Department of the Air Force.
ANACI	Access National Agency Check w/Written Inquiries – PSI that OPM conducts for the DoD PSP. The ANACI is conducted exclusively on civilians and is used to determine eligibility for federal employment, assignment to noncritical sensitive positions, and to grant Secret and Confidential security clearances.
CAF	Central Adjudication Facility – used here in the generic sense to refer to any office, regardless of its proper name, which is responsible for performing centralized adjudications for security eligibility.
CCF	Central Clearance Facility – the Department of the Army's CAF.
CCMS	Case Control Management System – DSS automated investigative process.
C-PR	Confidential – Periodic Reinvestigation
DCII	Defense Clearance and Investigations Index – a computer listing maintained by DIS, containing investigative and adjudicative information on DoD affiliated personnel.
DIA	Defense Intelligence Agency

DISCO	Defense Industrial Security Clearance Office – the section of DSS responsible for granting security clearances to DoD contractors.
DoD	Department of Defense
DOHA	Defense Office of Hearings and Appeals – the office responsible for making denial/revocation decisions for DoD contractors.
DONCAF	Department of the Navy Central Adjudication Facility
DSS	Defense Security Service – the only agency within the DoD authorized to conduct PSIs.
DSS-PIC	DSS Personnel Investigations Center – the section DSS responsible for controlling PSIs and PSI requests, and providing files and completed PSIs to requesters.
ENAC	Expanded National Agency Check – a NAC which has been expanded by DIS to resolve issues.
ENTNAC	Entrance National Agency Check – an investigation conducted exclusively for first term enlistees in the Armed Forces who do not require security clearance eligibility.
EO	Executive Order – an order issued by the President to create a policy and regulate its administration within the Executive Branch.
EPSQ	Electronic Personnel Security Questionnaire – an essential component of the CCMC; it provides data in electronic format.
FOCI	Foreign Ownership, Control, or Influence – PSI containing foreign ownership or control.
FOIA/PA	Freedom of Information Act/Privacy Act – Federal laws regulating access to and handling of information.

FPM	Federal Personnel Manual – a manual issued and updated by OPM and designed to administer the personnel management of civilian employees of the Federal government.
JS	Joint Staff
LAA	Limited Access Authorization – access authorized to non-U.S. citizens who require access to classified information in performance official duties.
LAC	Local Agency Check – an investigative check of local police departments, courts, etc., to determine whether the subject has been involved in criminal conduct. The LAC is a part of all PSIs except ENTNACs.
LOI	Letter of Intent – a letter from a CAF to a subject, notifying of the CAF's intent to deny/revoke security clearance/eligibility, and the reasons for the proposed action (see SOR).
NAC	National Agency Check – a component of all investigation conducted for the DoD PSP.
NACI	National Agency Check w/Written Inquiries – an investigation conducted by OPM to determine employment suitability for DoD civilians in non-sensitive positions.
NACLC	National Agency Check with Local Agency and Credit Checks – the lowest level PSI conducted by DSS for the DoD PSP for clearance purposes. It is used to grant Secret and Confidential clearances to military, contractors, and seasonal Employees
NSA	National Security Agency
OPM	The U.S. Office of Personnel Management – one of the successor agencies to the Civil Service Commission. OPM conducts NACIs and ANACIs on DoD civilians and a broad range of PSIs for other federal agencies.

PR	Periodic Reinvestigation – an investigation normally conducted every five years to update eligibility for Top Secret security clearances and/or assignments to critical sensitive positions.
PSI	Personnel Security Investigation – any investigation used to determine the eligibility of military, civilians or contractors to be enlisted, retained, hired, granted access to classified information or allowed to perform sensitive duties. The PSIs used in the DoD are: ENTNAC, NACI, NACL, ANACI, SSBI, C-PRs, PRs, S-PRs and SII.
PSP	Personnel Security Program – the DoD program established to ensure that only loyal, reliable and trustworthy people are granted access to classified information or allowed to perform sensitive duties.
ROI	Report of Investigation – report of the results of investigative inquiries. All PSIs and results from criminal and counter-intelligence agencies are ROIs.
SAP	Special Access Program – any program designed to control access, distribution and protection of particularly sensitive information established pursuant to EO 12356.
SCI	Sensitive Compartmented Information – classified information concerning or derived from intelligence sources, methods, or analytical processes which require special handling, per the Director of Central Intelligence.
S-PR	Secret - Periodic Reinvestigation
SSBI	Single Scope Background Investigation – the only PSI conducted by DSS for the DoD PSP for Top Secret and SCI duties. The SSBI covers a ten-year period.
SII	Special Investigative Inquiry – a PSI conducted by DSS to resolve specific issues raised in a previous PSI or raised subsequent to investigation and adjudication.
SOR	Statement of Reasons – a letter from a CAF to a subject, Notifying of the CAF's intent to deny/revoke security clearance/eligibility, and the reasons for the proposed action (see LOI).

TS

Top Secret – the highest level of security clearance in the DOD PSP. The other levels are Confidential and Secret.

WHS

Washington Headquarters Service

Introduction. . .

THE PERSONNEL SECURITY PROGRAM

As an adjudicator, you perform a critical role within the Department of Defense Personnel Security Program (DoD PSP). This course will introduce you to the DoD PSP and the role you play in it.

We will take a close at the PSP itself, what it is, why we have it and what its major elements are. In addition, we will give you a brief history of the PSP and review some of the major court decisions which have helped shape the program.

We will discuss the threats, both external and internal, which the DoD PSP was created to address. You will read about espionage efforts against the U.S., and actions taken to counter them.

The information presented in this course will help you place your role as an adjudicator in the overall DoD PSP, and underscore the importance of that role to national security.

In order to make the concepts we are trying to teach more concrete, we have created scenarios of certain situations from time to time for reinforcement.

So, welcome to the world of personnel security. We hope this course will be enjoyable, informative, and will prepare you for an exciting career as a personnel security specialist.

LESSON 1

Overview of the Personnel Security Program

In this lesson you'll be introduced to the Department of Defense Personnel Security Program and provided with an overview of the history of the program. You'll learn what the Personnel Security Program is, why DoD has it, and what its major elements are. You'll also learn where you, as an adjudicator, fit into the Personnel Security Program.

OBJECTIVES

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

- * State the purpose of the Personnel Security Program.
- * Define the meaning of National Security.
- * Identify the major elements of the Personnel Security Program.
- State the controlling regulation for the personnel security program.

READING ASSIGNMENT

Assignment 1:

DoD 5200.2R: Chapter 1: Section 3

Assignment 2:

"Recent Espionage Cases"

LEGAL AND HISTORICAL FOUNDATIONS OF THE FEDERAL EMPLOYEE PERSONNEL SECURITY PROGRAM

The notion of allegiance and trust is part of working for any government. It goes without saying that a government needs to be able to trust the people who put into effect its programs and policies. Our current notion of allegiance extends to our form of government rather than to the government of the day. That is, we require that federal employees swear an oath to uphold and support the constitution; we don't make them swear an oath of allegiance to the administration in power. It is not necessary for a loyal and trustworthy civil servant to be a supporter of the president in power. Even among federal employees, we welcome the diversity and strength offered by differing opinions, requiring only that they occur within the range offered by the constitution.

However, this was not always the case. Prior to the Civil Service Act of 1883, federal employees, even at the lowest levels, were political appointees. They were generally appointed as a reward for services to the party in power. This system (known as the Spoils System - as in "To the victor go the spoils") carries its own notion of allegiance. It requires allegiance to the political party and the party boss as opposed to the larger sense of allegiance to the Constitution. It also carries with it a presumption of allegiance. The employee is presumed to be loyal because in the past he has been loyal to the party and 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 is a powerful impetus for remaining loyal.

Because of the many abuses of the Spoils System (incompetent and corrupt public officials; civil servants who felt they were working for the party rather than for the American people, etc.), the Civil Service Act was passed in 1883, creating the U.S. Civil Service Commission. The Civil Service Act required that federal

employees be appointed on the basis of ability, after passing competitive exams. The Merit System, as it was known (because people held jobs on the basis of merit rather than favor) cured many of the abuses of the Spoils System. But it also created a concern about the loyalty of federal employees. Since they were no longer dependent upon party favor to keep their jobs, their allegiance could no longer be "bought" or necessarily even depended upon. The Hatch Act, passed by Congress in 1939, addressed that problem.

The Hatch Act represents the beginnings of the present day Personnel Security Program within the United States Government. The act was concerned with the allegiance of U.S. citizens to the United States and talked about membership in political parties or organizations or activities which advocate the overthrow of our constitutional form of government. Earlier, however, less structured programs date back to the Civil War when Allan Pinkerton formed the Secret Service with a major mission to detect disloyalty to the Union. Prior to the Civil War, the crimes of spying, lurking behind friendly lines, and giving aid and comfort to the enemy were dealt with summarily.

Civil Service applications prior to 1939 limited questions to those of character and general competence, political beliefs were considered outside the authority of the Civil Service Commission. President McKinley's Executive Order 101 in 1897 was the basis for the Lloyd-La Follette Act of 1912, which limited dismissal of employees to such reasons as will promote the efficiency of the service, required that employees be notified of the charges against them, gave them reasonable time to reply in writing, but required no hearing except at the discretion of the dismissing officer.

During World War I, at the suggestion of the Civil Service Commission, President Wilson issued a confidential Executive Order (EO) authorizing the removal of any

employee believed to be "inimical to the public welfare by reason of his conduct, sympathies, or utterances, or because of other reasons growing out of the war." The loyalty issue then became dormant until the turbulence of the thirties brought passage of the Hatch Act. The act ordered the immediate removal of any person advocating the overthrow of the United States by unlawful means.

During the 1940s, questions were added to applications for federal employment which asked about membership in subversive organizations and specifically mentioned Communist and German Bund organizations. Later versions mentioned Fascists. In 1941, President Roosevelt issued E.O. 8781 which required fingerprinting of every employee whose prints were not already on record and directed the Federal Bureau of Investigation to establish a system to check criminal records. The Civil Service Commission had been finger printing new employees only since July 1931.

The War Service Regulation II, issued in February, 1942, denied examination or appointment to anyone whose loyalty was in reasonable doubt.

The Secretaries of War and Navy and the Coast Guard were given power to summarily remove employees deemed risks to national security. The Congress placed the provision in appropriations bills that monies could not be used to pay the salary of any person advocating the overthrow of the government by force or violence.

Under War Service Regulation II, employment was refused to those actively associated with Nazi, Fascist, and Japanese groups, or were members of the Communist Party. The Civil Service Commission investigations staff conducted preappointment investigations of applicants, confronted them with derogatory information, provided for review, and forwarded adverse decisions to the head of the Commission for approval. The applicant could then appeal to the Commission's Board of Review. In the

spring of 1944, a full-time Loyalty Rating Board was established before which a person could appear in person if he/she wished. During this period the Commission began compiling a security index and a subversive file and the Department of Justice began to investigate charges of disloyalty.

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." The order was amended on April 28, 1951 to read, "The standard for the refusal of employment or the removal from employment in an executive department or agency on grounds relating to loyalty shall be that on all the evidence, there is reasonable doubt as to the loyalty of the person involved."

On April 27, 1953, President Eisenhower issued E.O. 10450 which is still in use and which states that ".. 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...". The phrasing is repeated in the Federal Personnel Manual and remains the standard for employment in the federal government.

The Federal Personnel Manual additionally establishes levels of position sensitivity which are the basis of the Personnel Security Program and will be discussed in detail in Lesson 2.

Executive Order 10450 and the requirements of the Federal Personnel Manual are implemented within Department of Defense by DoD 5200.2-R, DoD Personnel Security Program. Each component has its own regulation implementing the requirements of DoD 5200.2R.

THE MILITARY PERSONNEL SECURITY PROGRAM

Under the U. S. Constitution, the President is also the Commander-in-Chief. The inherent power of command he exercises is the basis for the military personnel security program. Military service is characterized by a high degree of personnel control and a compelling necessity for loyalty and obedience. The military program has as its objective the rejection or separation of persons whose membership in the Armed Forces does not meet the needs of national security, as expressed in Department of Defense Directives. DoD 5200.2-R is the present basis for the military personnel security program and is enforced by the Uniform Code of Military Justice. The President has the right to reject those individuals who are not suited for military service, including those who do not meet security standards.

The military security program was previously unified under Department of Defense by joint agreement of the service secretaries in "The Disposition of Commissioned and Enlisted Personnel of the Armed Forces of Doubtful Loyalty" issued October 26, 1948. The agreement basically implemented standards and procedures similar to those put into effect for civilians in the Executive Orders modified to fit the military system of jurisprudence. In 1956, DoD Directive 5210.9 established the military personnel security program and established the same loyalty standard as required for civilians - rejection or separation of persons "whose membership in the Armed Forces would not be clearly consistent with the interests of national security". The present DoD 5200.2-R requires that "based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States."

All three of the military services have established Personnel Security procedures which are controlled at the component level and which involve the input of security, legal, and personnel officials to insure that allegations are proved, individual rights are guaranteed, and the national security is served.

LEGAL AND HISTORICAL FOUNDATIONS OF THE INDUSTRIAL SECURITY PROGRAM

The Department of Defense Industrial Security Program (DISP) exists for the purpose of protecting classified information and material in the hands of Defense contractors. Other industrial security programs within DoD exist to provide physical protection to defense related facilities which don't have classified contracts but are deemed important to our national security. We will discuss only the program for determining the trustworthiness of persons involved in the protection of classified information and material held by industry.

While the Industrial Security Program is generally perceived to have been developed in response to the expanding World War II defense industry, it had its beginnings much earlier. The first formal legal effort to protect war materials was the Sabotage and Espionage Acts of 1917 which provided general protection under criminal law. A more specific law, the Air Corps Act of 1926 regulated the employment of aliens in aircraft plants. During the 1930s, various Army and Navy security regulations were imposed on contractors. In 1934, defense contractors were required to sign an agreement to follow security precautions and the prime contractor was made responsible for subcontractors. In 1939, the War Department (as the Department of the Army was known) required that classified information and material be marked with its classification level while in the hands of

defense contractors. During 1938-1940, the FBI conducted plant protection surveys in vital defense facilities. At the beginning of World War II, both the War Department and the Navy were administering industrial security regulations. To alleviate the confusion this caused, Navy allowed the War Department to take responsibility for the handling of aliens, control of subversives, fingerprinting, and personnel security procedures. Responsibility for the industrial security program was given to the Provost Marshal General of the Army.

The program included surveys and inspections of selected defense facilities and their armed guards, special alarm equipment, and other physical protection measures. Personnel records were checked. Personnel in sensitive positions were required to submit detailed security questionnaires and fingerprints were checked. In 1942, the War Department set up a program for the "Discharge of subversives from private plants and war department plants privately operated of importance to Army procurement." While lacking legal guarantees protecting employees' rights, the plan attempted to be fair and tried to find other employment for questionable persons. In 1948, the Army-Navy-Air Force Personnel Security Board (PSB) was created to grant or deny clearance for employment on aeronautical or classified contract work and to suspend individuals whose employment was inimical to the security interests of the United States. In October 1948, the Munitions Board Industrial Security Committee was approved to analyze the industrial security program and to develop procedures for the protection of classified information in the hands of industry.

From 1949 to 1953, the Industrial Security Division, within the Munitions Board, set up the major elements of the industrial security program.

By 1953 the Industrial Security Division had been renamed the Office of Industrial Security. During that

year the Armed Forces Industrial Security Regulation was issued by the Department of Defense to provide uniformity and consistency to the program. After a number of reorganizations the DISP is presently under the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and is managed by the Defense Security Service.

The DoD Industrial Security Program directive, DoD 5220.22-R (1985), is the basis for the current industrial security program throughout DoD and is based on E.O. 10865, "Safeguarding Classified Information Within Industry." The requirements of the Industrial Security Program are implemented within industry and DoD by DoD 5220.22-R. The program is operated by security executives within industry and Industrial Security Representatives from DSS.

COURT DECISIONS AFFECTING THE PSP

In addition to Executive Orders, Congressional legislation and Departmental regulations, court decisions have been a strong influence in shaping the PSP. These decisions result from subjects appealing unfavorable personnel security determinations (denials and revocations) to the federal courts. Court decisions have influenced the nature and scope of the program and have helped shape the way you do your job. Many of the aspects of the PSP that we now take for granted, such as the requirement to provide the subject with certain procedural benefits in a denial or revocation case (see Lesson 4, "Due Process") are a direct result of these decisions.

Why do you need to know about the court decisions that helped shape the program? After all, you're not a lawyer and the odds are you'll never argue a case before the Supreme Court. (Then again, you may - you never can

tell.) But there are several good reasons to be familiar with these cases. **Probably the most important reason is to impress upon you the potential consequences of your adjudicative determinations.**

The decisions you make as an adjudicator can have enormous impact on the subject and on the nation. The very fact that some personnel security cases (a small number to be sure, but important nevertheless) end up as cases being heard by the Supreme Court of the United States should serve to drive this point home.

The second reason has to do with being a professional adjudicator. As a professional working the field, there are certain things that you need to know - a body of knowledge with which you must be familiar. Included in that body of knowledge is the origins and sources of the PSP, such as significant court decisions.

Finally these cases have changed key aspects of the DoD PSP. As you'll see, DoD's due process procedures are a direct result of one of the court decisions. Some of these cases have affirmed the adjudication guidelines you use. Their impact on our program has been strong and can be expected to continue.

The cases we will discuss below represent the major court decisions affecting the DoD PSP. There have been other cases which affirmed many of the decisions or whose significance has been overtaken by time and events. In the interests of space, we are limiting our discussion to only the most important cases. (The citations show the plaintiff and defendant in each case. In Cole versus Young, Mr. Cole brought suit against the Secretary of DHEW, Mr. Young; in Clifford versus Shoultz, the Secretary of DoD, Mr. Clifford brought suit against Mr. Shoultz; etc.)

Cole v. Young

This case was brought in 1956 because Cole was dismissed from his position as a food and drug inspector for the Department of Health, Education and Welfare (DHEW). Cole was accused of close association with alleged Communists and contributing funds and services to an allegedly subversive organization. He was dismissed because his continued employment was not "clearly consistent with the interests of national security." The Court found in favor of Cole because the DHEW made no determination that Cole's position was a sensitive one in which he could adversely affect the "national security." That is, he occupied a non-sensitive position.

This case is significant because it limits the PSP to sensitive positions (when civilians are involved). It is also important because the court opinion includes a discussion of the dismissal of employees "in the interests of national security." That discussion mentioned examples of "security risks," who were security risks "... because of the risk they posed of intentional or inadvertent disclosure of confidential information." The example mentioned in the legislative history concerned alcohol abuse, and specifically off-duty alcohol abuse, because the individual "... may unintentionally or unwittingly, because of his condition, confide to someone who may be a subversive, secret military information..."

Greene v. McElroy

This case involved revocation of the security clearance of an aeronautical engineer who was vice-president and general manager of a defense contractor. Greene required a security clearance to be able to perform his duties with his company. DoD told Green that his security worthiness was suspect because of his alleged associations

with Communists. Green responded to the allegations and appeared, with counsel, before a four-member Board. Green testified on his own behalf, and presented witnesses to corroborate his testimony and to testify as to his good character. However, the Board relied on confidential reports containing statements adverse to Mr. Greene and denied him any opportunity to cross-examine the confidential sources. The Board issued a decision adverse to Mr. Greene, and he was subsequently discharged from his company after his security clearance was revoked.

Because of the revocation of his clearance, Greene couldn't find a job in his field. He sued the DoD. In 1959, the Supreme Court reversed the case on the grounds that neither the President nor Congress had authorized procedures which denied the subject the opportunity to confront and cross-examine the evidence against him. This case caused the establishment of due process procedures in the DoD PSP.

Adams v. Laird

In this 1969 case, the subject challenged the standard used to grant security clearances. EO 10865 (which authorizes the Industrial PSP) states that access to classified information is to be granted "only upon a finding that it is clearly consistent with the national interest to do so." The subject proposed that the standard should be that a clearance be denied only when the government can "point to a clear and present danger that a breach of security is actually threatened." The court disagreed, stating: "We know of no constitutional requirement that the President must, in seeking to safeguard the integrity of classified information, provide that a security clearance must be granted unless it be affirmatively proven that the applicant 'would use' it improperly."

The court further stated that the standard chosen by the President "... falls, in [the courts] view, within the range of rational choice vested in the President..."

This case is significant because it affirms the right of the PSP to deny or revoke a security clearance because of questions about the subject's loyalty, reliability and trustworthiness. If the subject had won this case, you would have to prove that a subject is disloyal, unreliable and untrustworthy before you could initiate a denial or revocation action. This would make your job immeasurably more difficult and could increase the risk to national security to an unacceptable level.

Service v. Dulles

This case involves a Foreign Service Officer who was improperly discharged by the Secretary of State after the Department's Loyalty Security Board found that he was neither disloyal nor a security risk, and the Deputy Under Secretary of State approved the finding.

The United States Supreme Court ruled that the Secretary's action violated the State Department regulations which said that approval of favorable findings by the Deputy Under Secretary are final and binding on the Secretary.

The significance of this case is that an agency must follow its own regulations, even when those regulations are more restrictive than the law requires. Failure to follow these regulations can cause the Court to decide a case in favor of the subject on the basis of procedural errors, without even looking at issues involved.

Dept. of the Navy v. Egan

This case involves a civilian employee of the Department of the Navy (DON) whose security clearance was denied in 1983. Subsequently, Egan was fired because there

were no non-sensitive jobs available for him to fill. He appealed the case to the Merit Systems Protection Board (MSPB), which after reviewing the case ordered that DON re-instate Egan and grant his clearance. DON appealed and, in 1987, the case was heard by the Supreme Court.

In 1988, the Supreme Court ruled that MSPB does not have the authority to review the substance of an underlying security clearance determination when reviewing an adverse action resulting from that determination. In other words, if someone is fired after losing his/her security clearance, MSPB can't look at the reason the clearance was denied or revoked.

This case is significant because it affirms that the granting or denial of a security clearance is a judgment call that is committed by law to the appropriate Executive Branch agency, in this case DON. The Court also stated that the standard that decisions must be clearly consistent with the interests of national security "indicates that security-clearance determinations should err, if they must, on the side of denials."

United States v. Yermian

This case involves a contractor employee who falsified information on his DD Form 48 in 1979. He was prosecuted for violation of Title 18, U.S.C. Section 1001, which states:

"Whoever, in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be fined not more than \$10,000 or imprisoned not more than five years, or both."

Yermian's sole defense was that he had no actual knowledge that his false statements would be transmitted to federal agencies.

The Supreme Court held that the language of the statute does not require that the individual know that the information falsified was given "in a matter within the jurisdiction of any department or agency of the United States..." Rather the "knowingly and willfully" language requires only that the individual knows that he is making "false, fictitious or fraudulent statements or representations" at the time he makes them. (That is, omissions due to mere forgetfulness or false statements made in a reasonable good faith belief that they are correct or accurate are not knowingly and willfully false or fraudulent under Section 1001.) The court pointed out that the statute does not require a specific "intent to deceive the Federal Government" nor an "intent to defraud the United States" nor a requirement that the individual know that the statements were in a matter within the jurisdiction of a federal agency.

This case is significant because falsification is one of the issues covered in the adjudication guidelines (See Lesson 5, "Adjudicative Issues").

Clifford v. Shoultz

This case began when Shoultz, a contractor employee, refused to answer specific questions from the Screening Board of the Industrial Security Clearance Review Office concerning his connection with the Cuban Communist Party. Shoultz already possessed a clearance.

In 1969, the United States Court of Appeals for the Ninth Circuit determined that suspension of a security clearance was permissible where an applicant refused to answer relevant questions posed by the Screening Board for

purpose of determining continuing eligibility for security clearance. In this case, the questions "[o]n their face were clearly relevant to a determination of his continued access to national defense information..." since they concerned his connection with the Cuban Communist Party and were directly related to the criteria. The subject argued that he should not be required to assist the Screening Board in its investigation. The Court disagreed, stating:

a. the investigative process is required to enable the DoD to carry out its responsibilities under Executive Order 10865;

b. the investigative process is not equivalent to a trial and, therefore, does not require the full range of procedural safeguards of a trial or quasi-judicial proceeding; and

c. any person investigated will be accorded procedural safeguards at a subsequent adjudicative proceeding under Executive Order 10865.

The subject argued that he should not be required to waive his Fifth Amendment right to avoid self-incrimination by answering questions posed by Screening Board in order to obtain or maintain a security clearance which is required for his job. But the Court stated that his interest in withholding factual information was outweighed by the Government's legitimate interest in "prevent[ing] classified information from falling into the hands of persons whose reliability and loyalty are not clearly established."

This case is important because refusal to answer or provide information is one of the issues covered in the adjudication guidelines (see Lesson 5, "Adjudicative Issues") and because it recognizes the government's overwhelming interest in protecting classified information.

Recap of the Court Decisions

The cases we have discussed have all had a major impact on the program. *Cole v. Young* and *Greene v. McElroy* are directly responsible for key aspects of the PSP: *Cole v. Young* limits the authority of the PSP to individuals who perform jobs which can affect the National Security; *Green v. McElroy* established the requirement for Due Process procedures when making adverse personnel security determinations.

The other cases discussed have served to affirm basic aspects of the program. *U.S. v. Yerman* and *Clifford v. Shultz* endorsed one of the adjudication guidelines. *DON v. Egan* and *Adams v. Laird* re-affirmed basic philosophies underlying the PSP: that errors, if any, must be on the side of the government and that disloyalty, untrustworthiness and unreliability need not be proved, only reasonably suspected.



WHO IS SUBJECT TO THE PSP?

John is a captain assigned as a war plans officer with the U.S. Army in Europe. Because of the extremely sensitive nature of the information his office handles, he has a Top Secret security clearance. Although John's married, his wife and children still live in the States. For

the last year, John has been having an affair with a German national. John's wife would divorce him if she found out about the affair.

Melinda is an electronics technician working for Acme Systems, Inc., a major defense contractor. She's working on a contract for the DoD, and will have daily access to state of the art technology being developed for a new weapons system. Because of this, Melinda needs a Top Secret security clearance. She also has a very expensive lifestyle, and for the last year has been getting deeper and deeper in debt. If she can't find some way to increase her income, she's going to have to file bankruptcy soon.

Sally has been hired to manage the computer center for a DoD agency. Although her job does not give her access to any classified information, it makes her responsible for the electronic transfer of millions of dollars a month in contract and payroll payments. On weekends, Sally usually smokes some marijuana and uses a little coke. The cocaine has been getting expensive lately, but so far she's been able to cover the cost.

Mike is a pipefitter working at a Department of the Navy shipyard. For the last few months, Mike's work crew has been busy refitting a battleship. Because he's working on the battleship and will have access to all of its plans, Mike needs a Secret security clearance. After work, Mike and his buddies like to go to a bar and have a few drinks. When he drinks, Mike talks a lot. In fact, his friends call him "Gabby" because he talks so much.

What do John, Melinda, Sally and Mike have in common? Each of them is affiliated with DoD - John is an Army officer, Melinda is a Defense contractor, and Sally and Mike are civil servants. Each has or will have special trust placed in him/her by the government - John has access to Top Secret war plans, Melinda will have access to Top Secret weapons design information, Sally will be

responsible for millions of dollars each month, and Mike will have access to the Secret plans of a battleship. Each has a character flaw or lifestyle which could make him or her a security risk - John is committing adultery and doesn't want his wife to know, making him susceptible to blackmail; Melinda is deeply in debt and looking for ways to raise her income, and selling classified information may be the way she chooses; Sally is using illegal drugs and may decide to use government money to finance her habit; and Mike's habit of talking too much when he drinks could give new life to the old saying "loose lips sink ships." The final thing that John, Melinda, Sally and Mike have in common is that they're all subject to the DoD Personnel Security Program.

WHAT IS THE PERSONNEL SECURITY PROGRAM?

The Personnel Security Program (PSP) is DoD's program to ensure that only loyal, reliable and trustworthy people have access to classified information or perform sensitive duties. The sole purpose of the PSP is to make sure that giving people access to classified information or allowing them to perform certain jobs is clearly consistent with the interests of national security.

WHAT IS THE NATIONAL SECURITY?

National Security is a concept that goes to the very heart of what it means to be a nation. Every nation must be able to defend itself, to ensure its own survival and the survival of its way of life. This is especially true of a country like ours, which was founded on certain principles and which is dedicated to maintaining certain freedoms and rights for its people. This ability of the nation to defend itself is one aspect of national security.

National defense.

Foreign relations.

The second aspect of national security is related to the first. It deals with the foreign relations of the United States. One way a nation can best defend itself is to manage its relations with other countries that they pose no threat to that nation's continued survival. It is for that reason that the foreign relations of the U.S. is the second half of the definition of national security.

These are the only two elements of national security. By definition, national security means the national defense and foreign relations of the defense and foreign relations of the U. S.

To ensure the national defense and foreign relations of the U.S., it is sometimes necessary that information related to national security be specially protected. This is because this information, if available to the wrong people, could damage the national security. That is, it could harm our national defense or foreign relations.

Information of this sort which requires special protection is known as national security information or *classified information*.

In the U.S., information is currently classified at three levels, "***Confidential***", "***Secret***", and "***Top Secret***." The level of classification is determined by the degree of damage to national security which could result from unauthorized disclosure.

"Confidential" is the lowest level of classification. It is used when unauthorized disclosure could reasonably be expected to cause ***damage*** to the national security.

"Secret" is the second level of classification. It's used when ***serious damage*** to national security could reasonably be expected to result from unauthorized disclosure.

When unauthorized disclosure can reasonably be expected to cause ***exceptionally grave damage*** to the national security, the designation "Top Secret"

is used. ***Top Secret (or "TS") is the highest level of classification.***

Some information is so sensitive that there must be accountability and control beyond those normally applied to "Confidential", "Secret", and "Top Secret" information. This information is usually part of a Special Access Program (SAP). SAPs are discussed in Lesson 2 and Lesson 4.

How information is designated as classified and who can designate it is tightly controlled within the government. Only a small number of senior officials (at present, fewer than 7,000 for the whole government) are authorized to originally classify information. This is to ensure that the government's need to protect information doesn't trespass too far on a free people's right to know information.

As an adjudicator, one of your primary functions is to determine whether people who need it, can be trusted with access to national security information.

When you decide they can, you authorize or grant a security clearance at one of the three classification levels. This means that when you grant a security clearance, ***you*** are saying that the subject can be trusted with information which, if given to the wrong people, can reasonably be expected to cause some degree of damage to the national security. This is a heavy responsibility and it makes you one of the guardians of the national security.

WHY DOES DoD NEED A PSP?

The reason DoD has a PSP is pretty simple - people aren't all the same. We all have different skills, different personalities and different levels of trustworthiness. You've experienced this in your own life. There are some people you'll trust with your confidences,

knowing that they won't repeat anything you say. There are some people you'd trust with your children or your power of attorney, knowing that your children and property are safe. And there are some people you wouldn't trust because you just can't be confident that they'll behave in a way consistent with that trust; you can't be sure of what they'll do.

This is the one fact that drives the DoD PSP - not everyone can be trusted. As the examples of John, Melinda, Sally and Mike show, there are a number of reasons someone might be untrustworthy. John is susceptible to blackmail because of his affair -in essence he could be forced to be untrustworthy. Melinda needs money badly and might decide to sell secrets to get it - she could choose to be untrustworthy. Sally's use of drugs is both illegal and expensive - it makes her behavior unpredictable and therefore, untrustworthy. Mike could reveal all sorts of classified information in his alcohol inspired babbling - he could be untrustworthy without even realizing it. If any of these things should happen, the results could be disastrous. By definition, these people could pose a risk to national security if they proved to be untrustworthy - they could endanger the national defense and the foreign relationships of the United States.

These characteristics which can undermine someone's trustworthiness are known as ***vulnerabilities***. They can make one vulnerable to outside exploitation, as in the cases of John and Mike. But they can also make one vulnerable to one's own weaknesses, as in Melinda's and Sally's cases. This means that although no one is trying to exploit the subject, he or she may betray the government's trust for personal gain or advantage. Either way, these vulnerabilities are a concern because of the threat which is constantly posed to national security by foreign nations and by dishonest U.S. citizens. Foreign nations pose the clearest, most readily identifiable threat to national security - we've all seen enough spy movies to realize this threat.

But an equally dangerous threat is posed by Americans who want the advantages (economic, industrial, etc) that illegal access to classified information can give them, or who simply want to get their hands on valuable government property, such as computers or even cash for their own personal gain.

It is the purpose of the PSP to minimize or eliminate this threat by clearing people who meet minimum levels of trustworthiness and have no more than an acceptable level of vulnerability.

MAJOR ELEMENTS OF THE PSP

What can the DoD do to eliminate or minimize this risk to the national security? What would you do in the same situation? You'd want to identify and limit those jobs which require access to classified information or some other special trust. You'd want to find out as much information about the people in these jobs as you could. Having collected the information, you would want to review it and decide if the people can indeed be trusted. And finally, you would want to check on those people to make sure they remain trustworthy. That's exactly what DoD does. In fact, the actions described above are the four major elements of the PSP, known respectively as designation of duties/positions, investigation, adjudication and continuous evaluation (see Figure 1-1).

MAJOR ELEMENTS OF THE PSP

***DESIGNATION OF DUTIES/POSITIONS**

***INVESTIGATION**

***ADJUDICATION**

***CONTINUOUS EVALUATION**

Figure 1-1

DESIGNATION OF DUTIES/POSITIONS

The first major element of the DoD PSP is designating duties and positions subject to the program. To be subject to the PSP, a position or duty must either require access to classified information or involve what are known as sensitive duties. Sensitive duties are those which require that a peculiar trust be placed in the individual performing the job. Your job as an adjudicator is a sensitive duty because of the high degree of trust placed in you, even if you never see classified information. All civilian positions are designated as nonsensitive, noncritical sensitive or critical sensitive. The PSP deals with the last two, noncritical-sensitive and critical sensitive. Military and contractor positions are less highly structured, but as you'll see in Lesson 2, they follow the same basic system.

The most important thing to realize at this point is that the primary focus is on positions and duties. People fall under the authority of the PSP only as occupants of sensitive positions or performers of sensitive duties.

INVESTIGATION

Once a person has been chosen to perform sensitive duties or have access to classified information, the next step is to collect information on him or her. This is done in two ways. The person (known as the subject, as in "the subject of the investigation") fills out certain forms about his or her background, similar to the forms that you filled out when you were hired as an adjudicator. These forms are used to pre-screen the subject, to weed out those who are clearly not eligible for access or to perform sensitive duties. They are also used as the basis for the Personnel Security Investigation (PSI) which will be conducted to make the final eligibility decision. A PSI is simply a check of subject's background to collect information to make this decision. There are a number of PSIs conducted for the PSP. Figure 1-2 is a listing of the different PSIs used by the program, and their common abbreviations. Which PSI is conducted depends on the level of classified information to which subject has access (Confidential, Secret or Top Secret, SCI) and the degree of sensitivity of his/her duties (Noncritical Sensitive or Critical Sensitive).

PSIs USED IN THE DOD PSP

Entrance National Agency Check.....	ENTNAC
National Agency Check w/Local Agency & Credit Checks.....	NACLCL
Access National Agency Check Plus Written Inquiries.....	ANACI
Single Scope Background Investigation.....	SSBI
Periodic Reinvestigation.....	PR
Secret PR.....	S-PR
Confidential PR.....	C-PR
Special Investigative Inquiry.....	SII

Figure 1-2

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 except the NACLCLs 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.

ADJUDICATION

Once the PSI has been completed, it has to be reviewed for completeness and for a determination of subject's eligibility for access or to perform sensitive duties. This function is called **adjudication**, and this is where you come into the process. As an adjudicator, your primary function is to review PSIs to determine if the subject can be trusted with classified information or to perform sensitive duties. This determination is made by applying the Security Criteria (para 2-200 of DoD Regulation 5200.2R) and the Adjudication Guidelines (Nov 98 Memo - Personnel Security Investigations and Adjudications). This sounds like a simple job, but as you already know, it's anything but that. Adjudication is essentially a process of predicting the future, based on the past. In this case, predicting subject's future behavior and trustworthiness based on his or her past behavior and trustworthiness. It requires a detailed knowledge of the DoD PSP as well as broad general knowledge and a strong measure of common sense. Adjudication is one of the most important elements of the PSP, for if a bad job is done here, everything else will have been in vain. Lessons 4 and 5 deal with adjudications and your responsibilities as an adjudicator.

CONTINUOUS EVALUATION

Once the adjudication has been made and the subject has been granted access to classified information or allowed to perform sensitive duties, the process is over and we go on to the next subject, right? Wrong! As long as the subject remains in security status - continues performing sensitive duties or accessing classified information - he or she remains subject to the PSP. This post-adjudicative portion of the program is known as the Continuous Evaluation Program (CEP).

The underlying principal of the CEP is that people change. Most of these changes are in predictable, acceptable directions, but many times people change in unpredictable and unacceptable ways. John is an example of someone who has changed in unacceptable ways, in ways that make you question his continued trustworthiness.

The CEP, recognizing that people change, requires that everyone under the authority of the PSP be subject to a continuing assessment of their security eligibility. Although continuous evaluation is everyone's responsibility, it falls primarily to the employing activity, and as an adjudicator you are also involved. A good part of your time will be spent reviewing information on people who have already received favorable security determinations, but about whom new information is now known. These cases frequently lead to a revocation of security clearance or eligibility to perform sensitive duties.

A second aspect of the CEP is a result of the nature of PSIs. No PSI is capable of developing and reporting every detail about a subject's life. Occasionally a PSI will fail to develop existing information which could effect an adjudicative decision. If this information becomes known after a security clearance has been granted, the subject's case is again reviewed and adjudicated with the new information under the CEP. These cases will sometimes lead to revocation actions.

Along with adjudications, the CEP is one of the most important aspects of the PSP. Without a vital and functioning Continuous Evaluation Program, it is impossible for the PSP to do its job. We will discuss the Continuous Evaluation Program further in Lesson 6.

THE BALANCE OF INTERESTS

A major concern of our society is maintaining the delicate balance between the interests of the government and the interests of the individual. Maintaining this balance is a basic principal of our form of government, and is a constant theme in our history as a nation.

The PSP has to pay particular attention to this issue, to balancing these sometimes conflicting interests. Overemphasis on the interests of the government would undoubtedly make the nation more secure, but at what cost? The very thing our government was created to ensure, personal liberty and freedom, could be lost in the process. On the other hand, overemphasis on the interests of the individual would allow for the greatest degree of personal liberty and freedom, but put at risk the system which protects and guarantees them.

The balance between these interests requires a system built on compromises. The PSP reflects these compromises. Rather than aiming at eliminating completely the risk to national security, the PSP seeks to determine the *acceptable risks* to national security. As you will see in Lesson 3, limitations are placed on the government when conducting PSIs. There are certain practices that must be avoided, as they are too intrusive and do too much violence to individual rights. There are certain questions which are not normally asked in the course of a PSI for the same reasons. On the other hand, individuals who fall under the authority of the program agree to give up certain rights to privacy, so that PSIs can be conducted. They also give up a certain freedom of action, by agreeing to behave consistent with the security criteria.

These compromises are the essence of our form of government and of the PSP. Being aware of these compromises and of the delicate balance which requires them will help you understand both the applications and the limitations of the DoD PSP.

CONTROLLING REGULATION OF THE DOD PSP

The DoD PSP and its major elements are mandated and regulated by DoD Regulation 5200.2-R of January 1987. This regulation is commonly known as "the **2-R**." The 2-R establishes the DoD PSP and the various requirements which go into making up the PSP. It is the source document for your component's regulation governing your own implementation of the PSP. In addition to the **2-R**, there have been several regulatory changes instituted by Executive Order 12968 and the Nov 98 Memorandum - Personnel Security Investigations and Adjudications.

By the time you have completed this course, you should be intimately familiar with the program regulation and the subsequent executive order and memorandum and its various requirements.



THE THREAT TO NATIONAL SECURITY

As we saw earlier in this lesson, the DoD Personnel Security Program was created to protect the national security of the U. S. Here you'll learn about the threats to that national security.

As an adjudicator, it's your job to evaluate an individual's vulnerabilities and determine what risks they could pose to the national security if they were exploited. An understanding of the nature of the threats facing us is critical for you to do this job.

Here we'll discuss the most common vulnerabilities. You will see how these vulnerabilities have often been exploited to cause real damage to our national security. We'll also look at some of the indicators that someone is committing espionage.

Additionally, we'll look at the threats to national security, both external and internal; the major elements of each; and briefly discuss the recent changes in the external threat.

When we're finished, you should be able to answer the following questions:

- ◆ What is the most commonly exploited vulnerability?

- ◆ What are the major indicators that someone is committing espionage?
- ◆ What are the two general types of threats to the national security?
- ◆ What is the relationship between vulnerabilities and threats?

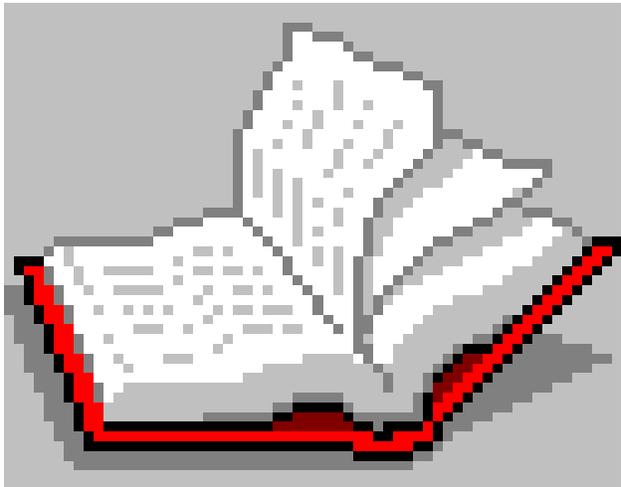
READING ASSIGNMENT

Attachment 2:

[Nov 98 Memorandum:](#)

Attachment 4:

[Recent Espionage Cases](#)



VUNERABILITIES

As you have learned, the purpose of the DoD PSP is to ensure that only trustworthy people have access to classified information or perform sensitive duties. To do this, we review a subject's background to determine if there are any circumstances, characteristics or weaknesses which would cause us to question his loyalty, reliability or trustworthiness. In the DoD PSP, we aren't concerned with

all of the weaknesses that people might have. After all, weaknesses are part of what make us human. We're only concerned with those which could pose an ***unacceptable risk*** to the national security.

Generally speaking, that means a weakness, characteristic or circumstance which could be exploited to cause the subject to act against the national interest. These weaknesses are known as "***vulnerabilities***" As you saw when you reviewed Attachment 1 of the Nov 98 Memo (attachment 2), the Adjudication Guidelines are a discussion of these vulnerabilities, and of the point at which a weakness becomes a vulnerability.

For a weakness to be a vulnerability, there has to be someone ready, willing and able to exploit it. This is what is known as the "***threat***" to national security. The threat is both external and internal.

The ***external threat*** is from foreign nations whose interests are different from, and often hostile to, our national interest.

The ***internal threat*** is from American citizens, businesses, etc., who are acting contrary to the national interest for their own personal or corporate gain.

Exploited Vulnerabilities

As you learned from your readings, the range of conduct, characteristics or weaknesses that can be exploited is almost endless. Everything from love to ethnic identification can be ***and has been*** exploited at one time or another. But you should also have seen that the most commonly exploited vulnerability is also the most basic -- ***GREED***. The reality is that most Americans who engage in espionage do it for the money. Some do it because they feel backed into a corner -- too many debts and too little

income. Others do it simply because their eyes are bigger than their pocketbooks. Figure 1-3 is a listing of espionage cases in which the sole or primary motive was either greed or indebtedness.

This information was drawn from the Recent Espionage Cases booklet which you will read as part of this lesson.

<i>THEY DID IT FOR THE MONEY</i>		
Ames	Baba	Barnett Bell
Brown	Buchanan	Cavanaugh Garcia
Haguewood	Hall	Harper
Helmich	Kunkle	Wolf
Miller	Mira	Moore
Morison	Ott	Pelton
Pollard	Richardson	Smith
Tobias	Walker, J.	Whitworth

Figure 1-3

Although greed is the most common (and the most commonly exploited) vulnerability, it isn't the only one. There are many other vulnerabilities which can be and too often are exploited. These vulnerabilities range from sex to having a grudge against the agency or government. Figure 1-4 shows some of the vulnerabilities which have been exploited in the past. This is not an all-inclusive list. All vulnerabilities are of significant concern, regardless of whether they have been exploited recently.

EXPLOITED VULNERABILITIES

- Financial (Ames)
- Violation of Security Regulations (Dedeyan)
- Foreign Connections/Hostage Situation (Humphrey)
- Ideology (Pollard and Dolce)
- Sex (Lonetree)
- Love (Scranage)
- Thrills (Nesbitt)
- Grudge against the Government/Agency (Moore, Davies, Richardson, Kunkle, Wolf)

Figure 1-4

It's not uncommon for several vulnerabilities to be present in a single individual. Typically, greed will be one of the vulnerabilities present. For instance, Pollard was motivated by both ideology and money; Kunkle, Wolf and Richardson by a grudge and by greed; etc.

The vulnerabilities we've discussed are only some of those which may be exploited. The DoD Adjudication Guidelines (Attachment 1 of the Nov 98 Memo) are a discussion of some of the most important areas of concerns. Each of these areas represents an area of potential vulnerability. (Figure 1-5 lists the vulnerabilities addressed in the Guidelines.)

AREAS OF POTENTIAL VULNERABILITY
From Nov 98 Memo "Personnel Security Investigations
and Adjudications"

- * Allegiance to the United States
- * Foreign Influence
- * Foreign Preference
- * Sexual Behavior
- * Personal Conduct
- * Financial Considerations
- * Alcohol Consumption
- * Drug Involvement
- * Emotional, Mental and Personality Disorders
- * Criminal Conduct
- * Security Violations
- * Outside Activities
- * Misuse of Information Technology Systems

Figure 1-5

This list, or any listing of vulnerabilities should never be considered as all-inclusive. Ultimately, we don't really know what makes some people betray their nation's trust and commit espionage. Until we do, we need to pay attention to any and all potential vulnerabilities.

KNOWN INDICATORS OF ESPIONAGE

Although we don't know *why* people engage in espionage, we do know some of the signs *that* someone is doing it. These are known as *indicators* of espionage. Although the presence of these indicators does not in and of itself mean that someone is committing espionage, they should cause you to give a case a closer look. This is especially true when a case has more than one indicator.

The first indicator is extensive foreign travel. Spies frequently need to meet with their controllers for

training, etc., and for obvious reasons they prefer to do this away from the eyes and ears of our nation's counterintelligence services. Traditionally, two foreign capitals have been especially popular for this purpose: Vienna, Austria and Mexico City, Mexico. Vienna was used to meet John Walker, Ronald Pelton and Edward Howard. Mexico City was used in the Christopher Boyce/Daulton Lee case. Aldrich Ames used Rome, Italy. This is why we require that people with clearances report all their foreign travel. If an individual has made periodic foreign trips, particularly to those locations, we may want more information to determine if there's a problem. (Remember, though, just because someone travels a lot, even to Vienna, Mexico City and Rome, it doesn't necessarily mean anything. American citizens are free, and indeed encouraged, to travel widely and often.)

Another common indicator of espionage is violation of security regulations. (Indeed, this is the one indicator that all spies have in common - they're all breaking the rules when it comes to security.) The violation may be the unauthorized removal of classified information, as in the case of Aldrich Ames, Michael Walker and, earlier, of his father. It may be bringing illegal cameras or other recording devices into restricted areas, as Christopher Boyce did. Another "common" violation is when someone tries to find out classified information to which he/she has no legitimate access or need to know. This was an unheeded sign that both Pollard and Morison were engaging in espionage. (Even if someone who violates security regulations isn't committing espionage, we're keenly interested. We'll discuss this further when you take the residential phase of this course.)

People who engage in espionage are often perceived as eager and even model employees. Unnecessary overtime and unusual work hours may be the sign of the workaholic, but they may also be the sign of a spy. They can give a spy the opportunity to copy material, browse through the files and possibly have access to material

when there isn't a need to know. This was seen in the Cavanaugh, Walker and Morison cases.

One of the most important indicators is what's known as *unexplained affluence*. This is when someone is living much better than he or she has any right to, given their known resources. Given that most people who spy do it for the money, it makes sense to look closely at this indicator. Frequently, spies can't control the urge to spend their money in a flashy, inappropriate way. John Walker had a plane; Jerry Whitworth's wife would meet him in a white Rolls Royce when his ship put in for shore leave; and Larry Wu-Tai Chin was known to be a high stakes gambler, a real high-roller. Aldrich Ames paid cash for a \$540,000 home and drove a new Jaguar automobile. Unexplained affluence isn't always due to spying; the person may have inherited money, won the lottery or have some other perfectly legal source of income. We need to find out, though. (We'll discuss unexplained affluence further in the residential phase of this course.)

THE THREAT

For vulnerabilities to be of concern to us, there has to be someone or something ready, willing and able to exploit it. This is known as the *threat* to the national security. Without a threat, vulnerabilities simply become idiosyncrasies, and of no legitimate interest to the government. In fact, without a threat, there is no need for the DoD Personnel Security Program - we exist solely to help protect the nation from the threat. This makes it critically important that you have some understanding of the nature of the threat. The national security of the United States is faced with two distinct threats - **the external threat and the internal threat.**

THE EXTERNAL THREAT

The external threat to the United States comes from other countries. No two countries have exactly the same national interests, even if they are close allies. Unfriendly nations, by definition, have competing national interests. This means that there is always a potential for conflict or disagreement between nations.

Because of this, virtually every nation on earth has an intelligence service to spy on other countries. These foreign intelligence services pose a continuing threat to the national security of the U.S.

During the Cold War, we thought only in terms of the threat posed by the intelligence services of the Soviet Union and its satellite states. This made it comparatively easy to understand and explain the threat. We only had to say "the USSR", and everyone knew what we meant, why we were worried, etc. Things are much more complicated now. The Soviet Union and the Warsaw Pact no longer exist. New countries are coming and going at a bewildering rate. (Figure 1-6 lists the now independent countries which made up the former Soviet Union.) This makes the threat seem more fluid and confusing than it used to. We have to pay much closer attention to the changing world situation, keep track of who is our friend, and who isn't. The old categories have changed.

<i>SUCCESSOR STATES TO THE USSR</i>		
Armenia	Kazakhstan	Russia
Azerbaijan	Kyrgyzstan	Tadzhikistan
Belarus	Latvia	Turkmenistan
Estonia	Lithuania	Ukraine
Georgia	Moldova	Uzbekistan

Figure 1-6

In fact, there really has been no significant change in the threat. The change has been in our *perception* of the threat. We are now paying more attention to that threat posed by nations other than the Soviet Union and its successor states. We're more awake to the fact that even friendly nations pose a potential threat to the national security. After reading the Recent Espionage Cases, you find that although the bulk of espionage against the United States has been conducted by or for the Soviet Union and its allies, they are by no means responsible for all of the espionage against us. Figure 1-7 shows some of the espionage cases which have involved other countries.

<i>ESPIONAGE AGAINST THE UNITED STATES</i>	
Stephan Baba	South Africa
Jonathan J. Pollard	Israel
Thomas Joseph Dolce	South Africa
Sharon M. Scranage	Ghana
Douglas Tsou	Taiwan
Waldo H. Duberstein	Libya
Michael H. Allen	Philippines
Albert T. Sombolay	Jordan

Figure 1-7

THE INTERNAL THREAT

The national security of the United States is threatened by more than the competing interests of other countries. It is also threatened by the selfish interests of individuals and corporations who deal with the government. The federal employee who abuses his position for personal profit; the contracting officer who reveals "confidential" bid information to competitors; and the nuclear and chemical weapons guard who drinks or uses drugs on the job are all posing risks to the national security every bit as real as the agent in the pay of

another country. The difference is that this risk is caused by dishonesty, greed and carelessness rather than disloyalty.

The internal threat is often overlooked, lost in the glare of the more glamorous "**external threat**". In many ways, it can be even more serious. When government officials and employees abuse their positions and the people's trust for personal gain, they not only endanger the national defense and foreign relations of the United States, they also put at risk the people's faith in the government itself. This damage can be much harder to make good than that caused by even the most successful spy.

SUMMARY

The Personnel Security Program exists in response to the threat to the national security. It focuses on those vulnerabilities in people which can be exploited. The most commonly exploited vulnerability is greed: most Americans who engage in espionage do it for the money. Many other vulnerabilities can be exploited, however, and we must pay attention to all of them. The DoD Adjudication Guidelines (Appendix I of the 5200.2-R) are essentially a discussion of some of the most common vulnerabilities.

Vulnerabilities are a concern because of the threat of "**exploitation**", causing people to act against the national security. That threat is both external and internal. The external threat is presented by the competing interests of other countries. Although we tend to think of only hostile nations as posing a threat, history has shown that any country, even an ally, can pose a threat if its interests are in competition with ours.

The internal threat is from American citizens and corporations who put their self-interest ahead of the national rest. The threat they pose is both real and serious.

Review Exercise

1. What are the four major elements of the Personnel Security Program?

1. _____ 3. _____
2. _____ 4. _____

2. What regulation has been mandated to control the DoD PSP?

3. In the PSP we are only concerned with those weaknesses which could pose an _____ to the National Security.

4. Unexplained affluence is a characteristic sign that may betray a spy.

- a. True
b. False

5. The purpose of the PSP is to ensure that only _____, _____ and _____ people have access to classified information or are allowed to perform sensitive duties.

6. Why does DoD need a Personnel Security Program?

7. *The underlying basis of the Continuous Evaluation Program is that people change over time.*

- a. True
- b. False

8. *The "threat" to National Security is caused by someone being vulnerable to exploitation.*

- a. True
- b. False

9. *Nov 98 Memo, attachment 1, reflects potential areas of vulnerability an adjudicator needs to be concerned with.*

- a. True
- b. False

10. *Vulnerabilities are exploitable weaknesses present in individuals.*

- a. True
- b. False

- 11. People fall under the authority of the PSP only as occupants of sensitive positions or performers of sensitive duties.**
- a. True
 - b. False
- 12. The PSP is concerned only with the threat posed by foreign intelligence service.**
- a. True
 - b. False
- 13. The National Security of the United States is threatened by more than the competing interests of other countries. It is also threatened by the selfish interests of individuals and corporations who deal with the U.S. Government.**
- a. True
 - b. False
- 14. The Soviet Bloc countries pose the only foreign intelligence threat to the U.S.**
- a. True
 - b. False
- 15. What is the relationship between vulnerabilities and threats?**
- a. They are the same thing.
 - b. Vulnerabilities exploit the threat.
 - c. Threats exploit vulnerabilities.
 - d. There is no relationship between them.

Solutions & References

1. *(Lesson 1, page 1-22)*
 1. *Designation of Positions/Duties*
 2. *Investigation*
 3. *Adjudication*
 4. *Continuous Evaluation*

2. *The DoD Regulation 5200.2R (Lesson 1, page 1-27)*

3. *unacceptable risk (Lesson 1, page 1-30)*

4. a. *True (Lesson 1, page 1-34)*

5. *reliable, trustworthy and loyal (Lesson 1, page 1-18)*

6. *Because all people are not equally trustworthy. (Lesson 1, page 1-20)*

7. a. *True (Lesson 1, page 1-25)*

8. a. *True (Lesson 1, page 1-30)*

9. a. *True (Lesson 1, page 1-32)*

10. a. *True (Lesson 1, page 1-30)*

11. a. *True (Lesson 1, page 1-23)*

- 12. b. False (Lesson 1, page 1-37)**
- 13. a. True (Lesson 1, page 1-37)**
- 14. b. False (Lesson 1, page 1-36)**
- 15. c. Threats exploit vulnerabilities. (Lesson 1, page 1-35)**

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:

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 (NACLIC) 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).

Types of PSIs

PSI

- National Agency Check with Local Agency and Credit Checks (NACLC)
- Access National Agency Check with Written Inquiries (ANACI)
- Single Scope Background Investigation (SSBI)
- Periodic Reinvestigation (PR)
- Secret Periodic Reinvestigation (SPR)
- Confidential Periodic Reinvestigation (CPR)
- Special Investigative Inquiry (SII)

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.

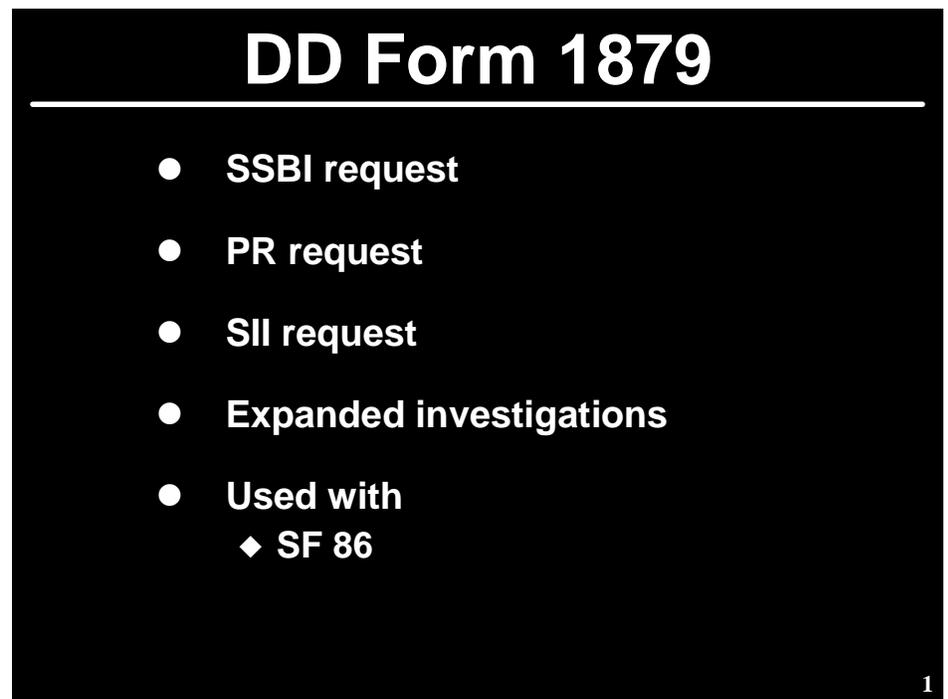


Figure 2-5

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, NACLIC, 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, NACLIC 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 ASSIGNMENTS

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

DoD 5200 2R Chapter 3: Sections 3 & 5

DoD 5200 2R Chapter 7: all

DoD 5200 2R 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)

LESSON 3

Personnel Security Investigations

As an adjudicator, you will spend most of your time reviewing and adjudicating Personnel Security Investigations (PSIs). This lesson addresses some of the most important aspects of the PSI and the agencies which conduct them.

Here you will learn about DSS and OPM, the two agencies which conduct PSIs for the DoD PSP. We will discuss the major duties these agencies have under the DoD PSP, and the offices which are responsible for performing those duties. We will also discuss the jurisdictional limits under which DSS and OPM operate.

After discussing the investigative agencies, we will look at the PSIs themselves. You will learn about the types of PSIs authorized in the DoD PSP, and how each PSI is used. You will also learn the components of each PSI and the minimum investigative requirements of each.

Finally, we will look at the new investigative forms used for each PSI and discuss the major uses of each form and learn about some of the common problems with each type of PSI. We will discuss the reasons for these problems and the consequences they have for PSIs and the DoD PSP.

This information will help you to understand the investigative process, which is one of the major elements of the PSP. It will also expand your knowledge of the PSIs which play such a critical role in the adjudicative process.

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

- ◆ Which investigative agencies are authorized to conduct PSIs for DoD?

Which PSI does each agency conduct?

What are the authority and responsibilities of investigative agencies for conducting investigations?

What are the jurisdictional limits of each investigative agency?

What offices within DSS are involved in the personnel security program?

What offices within OPM are involved in the personnel security program?

What are the topics about which DSS investigators may not usually inquire?

What are five investigative techniques that DSS investigators may not use?

READING ASSIGNMENTS

DoD 5200.2R: Chapter 2: Section 4, Para.2-504

10 Nov 98 Memo "Personnel Security Investigations and Adjudication"

22 Aug 00 Memo "Personnel Security Clearance Investigations"

How to Read Credit Reports

INVESTIGATIVE AGENCIES

As you know, the DoD PSP applies to a broad range of personnel - military, civilians and contractors. Because of this varied population, DoD uses PSIs from different investigative agencies.

“DSS and OPM are the only agencies authorized to conduct PSIs for the DoD PSP”

The Defense Investigative Service (DSS) and U. S. Office of Personnel Management (OPM) are the only agencies authorized to conduct PSIs for the DoD PSP. This means that when a DoD activity requests a PSI on one of its personnel, the PSI must be requested from either DSS or OPM. (If a subject was previously investigated by another agency, the FBI for instance, that PSI may satisfy the investigative requirements for DoD. Although DSS and OPM are both authorized investigative agencies for the DoD PSP, they don't conduct the same investigations for our program. Each has its own area of responsibility in the program.

Which agency is asked to conduct the PSI depends upon which PSI is needed and the category of the individual being investigated (military; civilian; contractor). Refer to attachment 5 (Memorandum August 22, 2000 -“Personnel Security Clearance Investigations”) for further guidance.

THE AUTHORITY, RESPONSIBILITIES AND JURISDICTION OF OPM

The first investigative agency we'll discuss is the U.S. Office of Personnel Management. We're all familiar with OPM as the government's personnel agency. You may be less familiar with its role in the federal government's personnel security program.

The PSP for the Executive Branch is authorized by Executive Order (EO) 10450, signed by President Eisenhower in 1953 and amended by EO 12968 in August 1995. EO 10450 gave primary responsibility for the PSP to the now defunct U.S. Civil Service Commission (CSC). As one of the successor agencies to CSC, OPM has

inherited these responsibilities. It is under this authority that OPM is one of the investigative agencies for the DoD PSP.

OPM is charged with the responsibility of conducting NACIs and ANACIs on all selected civilian personnel or occupants of non-sensitive and non-critical sensitive positions. The NACI investigation is designed to determine suitability for employment with the Federal government. Because of this, OPM is responsible for investigating all **civilians** selected for non-sensitive and for non-critical sensitive positions and Secret and Confidential clearances in the DoD. NACIs are only conducted on those individual designated to occupy Non-sensitive position within DoD. The ANACI is the minimum investigation conducted on DoD civilian personnel within the DoD PSP. The ANACI investigation serves as the basis to grant Secret and Confidential clearances to civilians within DoD. OPM has also been solicited to assist DSS with conducting various other types of PSI within the DoD PSP.

Although the Executive Order gives OPM the responsibility to investigate all competitive service employees of the Executive Branch, it also allows OPM to delegate this authority to other agencies. OPM and DSS have an agreement in which OPM delegates to DSS the authority to conduct all PSIs for the DoD except the NACI and ANACI.

OPM's jurisdiction is limited by this agreement with DSS. While OPM investigates all the personnel of some agencies, it is limited to just a small slice of the DoD population. However, OPM retains an oversight jurisdiction under its EO 10450 and EO 12968 authority, and has overall program responsibility for the Executive Branch PSP.

ORGANIZATIONAL ELEMENTS OF OPM

There are two major organizational elements of OPM which pertain to the DoD PSP. They are the **Office of Federal Investigations (OFI)** and the **Federal Investigations Processing Center (FIPC)**. Figure 3-1 shows a chart representing this organizational set-up.

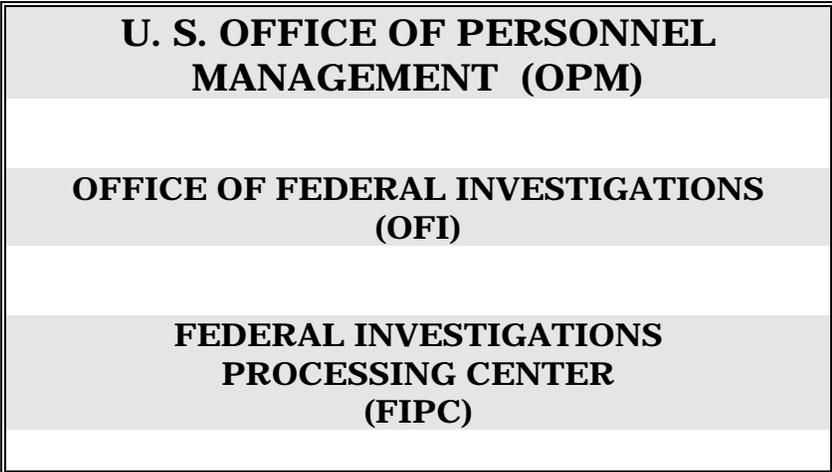


Figure 3-1

OFFICE OF FEDERAL INVESTIGATIONS (OFI)

OFI is the section within OPM which has the responsibility for discharging OPM's security functions. OFI conducts all OPM run investigations and maintains the inter-agency agreements which allow DSS and other agencies to conduct PSIs. This office also works with other federal agencies to determine the investigative elements of the different types of PSIs.

“OFI is responsible for discharging OPM’s security functions.” The OFI is responsible for making a continuing study of how the PSP is run by Executive Branch agencies, to insure that the requirements of EO 10450 and EO 12968 are being met. This is done by the Security Appraisals Branch of OFI.

The Office of Federal Investigations also maintains the Security/Suitability Investigations Index (OPM SII), which is a computer index of all PSIs conducted by all agencies under the authority of EO 10450 and EO 12968. (**Note:** Don’t confuse the OPM SII with the DSS investigation, the SII.)

FEDERAL INVESTIGATIONS PROCESSING CENTER (FIPC)

FIPC is an office within the Office of Federal Investigations. It is located in Boyers, PA, and is routinely referred to as simply "Boyers" or "the NACI Center". It’s known as the NACI Center because the main function of the FIPC is running all the NACIs and ANACIs for the federal government. This office initiates the investigations, reviews the results, arranges for additional investigation, when necessary, and forwards the completed NACI/ANACI to the requesting agency. The FIPC is responsible for sending requesters, such as DSS or the CAF, copies of previously completed OPM investigations. The FIPC is the organizational element of OPM which you will have the most contact as it is the one which is the most involved in the DoD PSP.

THE AUTHORITY, RESPONSIBILITIES AND JURISDICTION OF DSS

The Defense Security Service (DSS) is the investigative agency with which you'll deal most often. DSS was established in 1972 to serve as a single, centralized personnel security investigative service for the DoD. Before that, each of the military departments (the Army, Navy and Air Force) conducted its own PSIs. This led to a lot of inconsistency and duplication of efforts. DSS was created to eliminate these problems.

DSS is responsible for conducting PSIs on all DoD affiliated personnel.

A person is considered to be affiliated with DoD if he/she is in the Armed Forces or National Guard; employed by or contracting with DoD; living or working on any DoD installation or facility; or applying for any of the above.

“DSS jurisdiction is limited to the 50 states, the District of Columbia and Puerto Rico.”

DSS has overall responsibility for the Defense Industrial Security Program (DISP). This includes responsibility for granting security clearances to contractors working with classified DoD information.

DSS jurisdiction is limited to the 50 states, the District of Columbia and Puerto Rico. When a PSI requires investigation in areas outside of DSS jurisdiction (for example, when investigating a military member stationed overseas), DSS requests that one of the military departments or some other federal agency conduct the necessary investigation. Even in these cases, however, DSS retains control of the PSI and is responsible for directing the investigation.

DSS can only collect info on persons or organizations which are affiliated with DoD.

The second major jurisdictional limit on DSS (and on all DoD components) is a requirement for DoD affiliation. DoD policy prohibits DSS from collecting, reporting, processing or storing information on persons or organizations which are not affiliated with DoD. The only exception is when such information is essential to the DSS mission. An example of such “essential” information is the phone number of the local police department or credit bureau.

DSS must refer allegiance cases to the FBI or military CI.

Even when an investigation falls under DSS jurisdiction in terms of geography and affiliation, there is a third limit on DSS jurisdiction which may apply. As you read in para 2-401 of the regulation, there are certain instances when DSS must refer an investigation to other investigative agencies. Generally speaking, this happens when the investigation becomes what is known as an "allegiance case." (Allegiance cases will be discussed later) These cases are the exclusive territory of the FBI and the military department counterintelligence (CI) agencies - the Army Intelligence and Security Command (INSCOM), the Naval Investigative Service (NIS), and the Air Force Office of Special Investigations (AFOSI).

ORGANIZATIONAL ELEMENTS OF DSS

The Defense Investigative Service is divided into two major sections, reflecting its two missions. The Directorate for Investigations is the section responsible for conducting all PSIs for the DoD. The Directorate for Industrial Security is responsible for managing the Defense Industrial Security Program (DISP). Both of these Directorates are further divided into offices which you'll deal with on a regular basis.

DIRECTORATE FOR INVESTIGATIONS

The Directorate for Investigations is the section of DSS that has the greatest involvement in the DoD PSP. As an adjudicator, you see their work every day in the form of PSIs, and you interact with them daily via the DCII. Because of this, you need to know, in general terms, about their organizational structure.

PERSONNEL INVESTIGATIONS CENTER

***PIC is the
Personnel
Investigations
Center.***

When a DoD activity requests a PSI from DSS, the request is sent to the **Personnel Investigations Center (PIC)** in Linthicum, Maryland. The PIC is responsible for scheduling and controlling all PSIs conducted by DSS. The PIC conducts the National Agency Check (NAC), which is both an integral part of all other PSIs and a PSI in its own right.

Additionally, the PIC runs credit checks on all PSI submitted for clearance purposes. All other investigative elements are done by DSS investigators in the field at the direction of the PIC.

The PIC is also responsible for sending previous investigations to requesters. For instance, a CAF may need to review a PSI completed several years ago. The PIC would be requested to obtain a copy of the investigation and send it to the CAF.

PIC also maintains the DCII.

The final major responsibility of the PIC is maintaining the Defense Clearance and Investigations Index (DCII). The DCII, a computer listing of investigations conducted by DoD, is maintained and updated by the PIC.

Management of the this database is one of the most important PIC functions. A check of the DCII is an element of all NACs and increasingly the DCII is the central repository for adjudicative as well as investigative information.

DIRECTORATE FOR INDUSTRIAL SECURITY

DSS is in charge of the DISP.

The Directorate for Industrial Security is the section of DSS which manages the DISP. It is responsible for all aspects of Industrial Security, including personnel security. The only program element of the Directorate for Industrial Security that has any bearing on our program is the Defense Industrial Security Clearance Office (DISCO).

DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE (DISCO)

DISCO is responsible for granting security clearances to contractors.

The Defense Industrial Security Clearance Office located in Columbus, OH. **DISCO** is the central adjudication facility for the Industrial Security Program and is responsible for reviewing PSI requests from contractors and for granting security clearances to defense contractors. Unlike the other CAFs, DISCO is not responsible for denying or revoking security clearances. When cases are likely to lead to denial or revocation action, DISCO refers them to the Defense Office of Hearings and Appeals (DOHA) which is part of the Defense Legal Services Agency, under the DoD Office of the General Counsel. DISCO's authority is restricted to making favorable decisions only.

PROHIBITED INVESTIGATIVE TECHNIQUES

When conducting PSIs, DSS relies almost exclusively on personal interviews and record checks to develop information. Other investigative techniques which are freely used by CI and criminal investigators are forbidden to DSS. This is because of the balancing act between the government's need to know and the person's rights to privacy which we discussed in Lesson 1, "Overview of the Personnel Security Program."

Because of this, DSS is barred from using investigative techniques that are unnecessarily intrusive or which may violate the subject's constitutionally protected rights. DoD regulation requires that DSS "refrain from using, under any circumstances," these techniques. Figure 3-2 shows a list of prohibited techniques.

PROHIBITED TECHNIQUES

- Using mail covers (reviewing incoming and outgoing mail)
- Conducting physical surveillance
- Conducting photographic surveillance
- Conducting physical searches
- Using voice analyzers
- Inspecting trash
- Using paid informants
- Using wiretaps (of telephones)
- Using eavesdropping devices (hidden microphones, etc.)

Figure 3-2

PROHIBITED AREAS OF QUESTIONING

DSS may collect only information which is both relevant and necessary.

In addition to the prohibited investigative techniques DSS usually avoids asking questions about certain very personal areas of a subject's life. DSS may collect only information which is both relevant and necessary. The overall requirement is that an investigation should collect only as much information as is **relevant** and **necessary** to make a personnel security determination.

The critical words there are "relevant" and "necessary". If a question can't be reasonably expected to produce information that is **both** relevant and necessary to the issue at hand, there is no point in asking it. Thus a DSS agent may not ask a subject about his or her religious beliefs or political affiliation unless the question passes both tests. Of course, this will vary from case to case, but only in unusual circumstances (such as when the subject is a member of the Communist Party) would such questions be acceptable or even tolerable. Figure 3-3 shows a listing of the general areas of questioning which a DSS agent must avoid.



The DSS Manual for Personnel Security Investigations (January 1993) gives examples of questions which a DSS agent normally may not ask.

AREAS OF QUESTIONING GENERALLY AVOIDED

Religious beliefs and affiliations

Beliefs and opinions in racial matters

Political belief and affiliations (unless
subversive)

Opinions about legislative policies or Supreme
Court decisions

Membership in a trade union or fraternal
organization

Sexual Orientation

NOTE: This list is not all inclusive. If a line of questioning is not relevant and necessary, it should be considered prohibited.

Figure 3-3

These prohibitions are general in nature and are not absolute. There are instances, depending upon the information developed in a case, when such questions become appropriate and necessary.

For instance, while a subject would not normally be asked, "What is your net worth?" That question becomes both relevant and necessary if an issue of financial irresponsibility or unexplained affluence is developed. The acid test is whether the question, or line of questioning, is both relevant and necessary. If so, the question must be asked. If not, the question may not be asked.

SUMMARY

DSS and OPM are the only agencies authorized to conduct PSIs for the DoD PSP. OPM and DSS have joint responsibility for conducting investigations on certain civilian, military, and contractor personnel with the DoD PSP

OPM draws its authority from EO 10450, as one of the successor agencies to the Civil Service Commission. In addition to conducting investigations, OPM has certain management and oversight responsibilities for the entire Executive Branch PSP.

The Federal Investigations Processing Center (FIPC) of the Office of Federal Investigations (OFI) is the OPM office responsible for conducting the NACI and ANACI.

DSS is authorized by DoD to act as the only personnel security investigating service in the DoD. By agreement with OPM, DSS has received delegated authority to conduct PSIs. DSS' jurisdiction extends to the 50 states, the District of Columbia and Puerto Rico, and is limited to DoD affiliated personnel. When an investigation becomes a loyalty case, DSS loses jurisdiction to a CI investigating agency. DSS had two major missions - Investigations and Industrial Security. DSS agents are assigned to the Investigations Directorate where they conduct PSIs under the direction of the Personnel Investigations Center. PSIs for contractors are adjudicated by DISCO, which is part of the Industrial Security Directorate. When conducting PSIs, DSS must avoid unnecessarily intrusive techniques and ask only questions which are both relevant and necessary.

THE PERSONNEL SECURITY INVESTIGATION

Now we will begin our discussion of the PSI. You will learn what PSIs are used in the DoD PSP and the uses of each. You will also learn the minimum investigative requirements (scope) of each PSI.

Finally, we will look at the subject interview. You will learn when the subject interview is included as part of a PSI and why so much reliance is placed on the subject interview. Since the PSI is the major tool you will use as an adjudicator, this information will prepare you to review and adjudicate investigations.

WHAT IS A PERSONNEL SECURITY INVESTIGATION?

A personnel security investigation (PSI) is an inquiry into someone's background, lifestyle and personal history. PSIs are used to collect information to determine if a person can be trusted with sensitive duties or classified information. As an adjudicator, the lion's share of your time is spent reviewing PSIs and deciding whether the subject can be trusted. Because of this, you need to know as much as possible about PSIs - what they are, what they're used for, and so on. The more you know about PSIs, the more effectively and efficiently you can do your job.

Why Do We Use PSIs?

- Means to gather information about a person
- Used to evaluate eligibility
 - ◆ Access
 - ◆ Sensitive duties
 - ◆ Suitability for service
 - ◆ Other programs



3

Figure 3-4

PSIs AUTHORIZED IN THE DOD PSP

Because the DoD PSP has to meet the needs of a large and diverse population (military members, civilian employees and contractors), it relies on a wide range of PSIs. Each PSI is highly specialized and differs from each other PSI. They differ in their uses and in their comprehensiveness. One is an exhaustive inquiry into the last seven (7) years of the subject's life, while another simply runs the subject's name through a few government computer systems.

"...a PSI conducted for one purpose may not be sufficient for another..."

These differences mean that PSIs are not interchangeable; that a PSI conducted for one purpose may not be sufficient for another purpose. As a general rule of thumb, however, a higher investigation (a more comprehensive one) will always be able to take the place of a lower investigation (a less comprehensive one); but a lower investigation can never take the place of a higher one. This means that if

a former military member with a valid SSBI on record is hired as a civilian employee, there is no need to request an NACI or ANACI. The SSBI is higher than an NACI and ANACI (that is, it's a more comprehensive investigation) and can substitute for it.

Why Do We Use PSIs?

- Uniform collection of *important* and *relevant* information about the person
- The more sensitive the duties, the more comprehensive the PSI
- The greater the risk, the more we want to know about the person
- The *potential* for damage is greater with Top Secret than Confidential



4

Figure 3-5

However, if the military member only has a valid NAC on record, an NACI or ANACI must be requested. The NAC is lower than an NACI and ANACI (that is, it's a less comprehensive investigation) and cannot substitute for it.

It is important to remember that there are only three investigations approved for the initial issuance of a security clearance eligibility. They are the SSBI, ANACI, and NACLIC.

The PSIs authorized in the DOD PSP are shown in Figure 3-6, in order of highest (or most comprehensive) to lowest (or least comprehensive), except the SII, which is shown at the end. This is because the SII, being an issue-oriented investigation, can never replace another PSI.

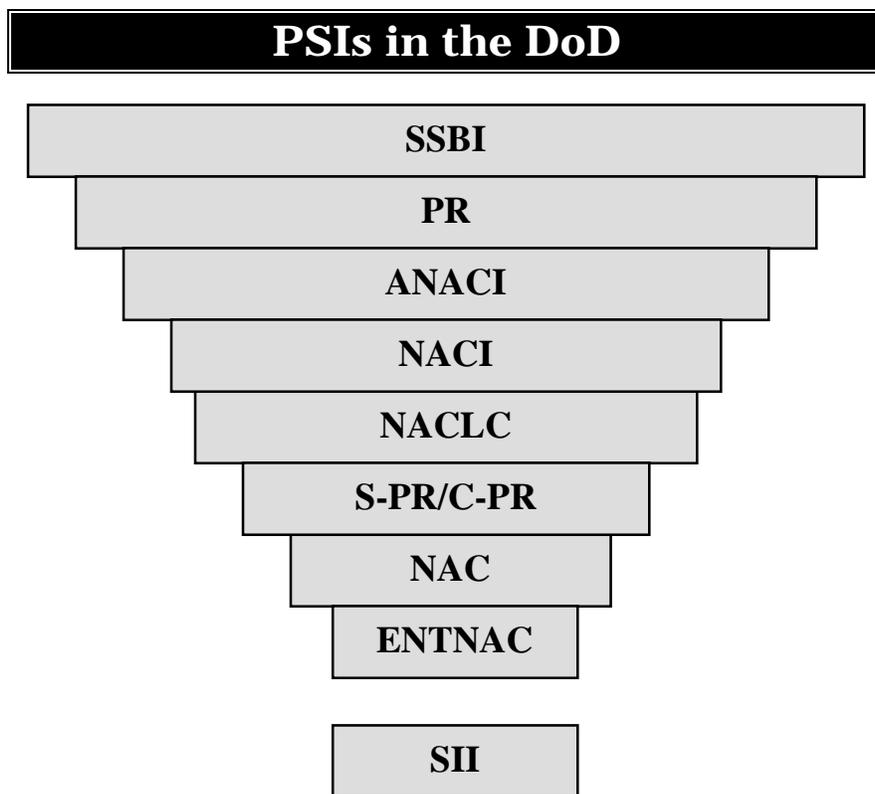


Figure 3-6

TYPES OF PSIs AND THEIR USES

Investigative requirements are different for each group of personnel

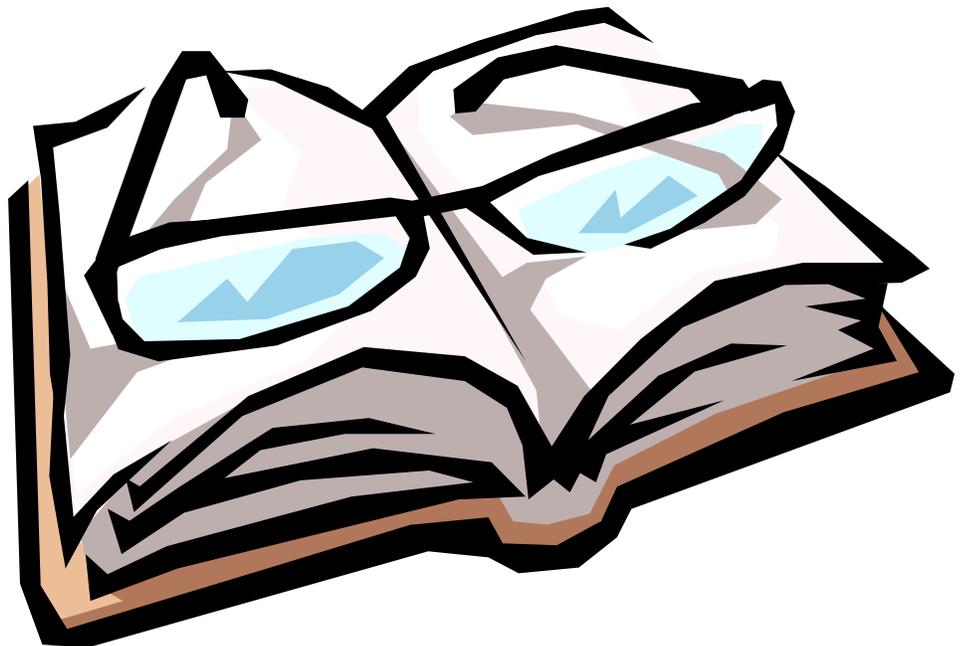
As you will read in Chapter 3 of the regulation, different levels of clearances and sensitive duties have different investigative requirements. In fact, it's not enough just to know what level of clearance is needed before you decide which PSI is required. You also need to know whether the subject is a civilian employee, a military member or a contractor. The investigative requirements are different for each group of personnel, and even for different categories of people within each group. **Note: Please refer to the Nov 98 memo-Pers. Secu. Inv. & Adjud.**

For instance, first term enlistees cannot be granted a secret clearance with an ENTNAC as all military members requiring a Secret clearance must be the subject of a NACL. However, an ENTNAC is sufficient for accession in some branches of the military.

These differences are a result of the history of the PSP. EO 10450 established the PSP for civilians; EO 10865

established it for contractors; and DoD 5200.2R authorizes the PSP for military members. Each of these sources set up different investigative requirements for the personnel under its authority. The result is that although DoD has only one PSP, it's a little bit different for each category of personnel. Figure 3-7 contains a ready reference chart for the major uses of each type of PSI.

In addition, each PSI is shown in Figures 3-8 through 3-15, with a complete listing of its uses and the categories of personnel to which it applies. The information in these figures is a consolidation of material presented in Chapter 3 of the Regulation.



PSIs AND THEIR USES AT A GLANCE

ENTNAC: Accessions for Army & Marine Corp military members not requiring access to classified and/or sensitive information

NAC: Contractors requiring access to restricted unclassified areas, NAF POT, Summer Hires

NACLCLC:	Military & Contractor personnel requiring Secret or Confidential Clearances. Accessions for Navy and Air Force military members
NACI:	Civilians only – Nonsensitive positions
ANACI:	Civilians only – Noncritical-sensitive positions Confidential and Secret Clearances
SSBI:	Military, Contractors, Civilians Critical-Sensitive Duties LAA Top Secret Clearance Special Access Programs Investigative Duties
PR:	Military, Contractors and Civilians Critical Sensitive Duties Top Secret Clearance
S-PR:	Military, Contractor and Civilians requiring Secret Clearances
C-PR:	Military, Contractor and Civilians requiring Confidential Clearances
SII:	Military, Contractors, Civilians – Issue Resolution

Figure 3-7

ENTNAC

ENTRANCE NATIONAL AGENCY CHECK

- Military Accessions (Army & Marine Corp) not requiring access to classified information
- Access to restricted areas and sensitive information or equipment
- Transportation of Category I and II Arms Ammunition and Explosives (AA&E)
- ADP III duties
- Interim Top Secret clearance if the other requirements have been satisfied

Figure 3-8

NATIONAL AGENCY CHECK (NAC)

- ◆ Employment in a Non-Appropriated Fund Position of Trust (NAFPOT) & Summer Hire
- ◆ ADP III duties
- ◆ DoD building passes in the National Capitol Region
- ◆ Contract personnel not requiring classified access
- ◆ DoD employees serving as customs inspectors
- ◆ Red Cross/USO personnel assigned with the Armed Forces overseas
- ◆ Access to restricted areas and sensitive information or equipment
- ◆ Interim Top Secret clearance, if the other requirements have been satisfied.

Figure 3-9

NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES

- ◆ Conducted on civilians employees only
- ◆ Appointment to Non-sensitive positions
- ◆ ADP III positions
- ◆ Interim Top Secret Clearances, if the other requirements have been satisfied

ACCESS NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES

- ◆ Conducted on civilian employees only
- ◆ Appointment to Noncritical-Sensitive positions
- ◆ ADP II positions
- ◆ Nuclear PRP Controlled positions
- ◆ NATO Confidential and Secret
- ◆ Secret and Confidential clearances
- ◆ Interim Top Secret Clearances, if the other requirements have been satisfied

Figure 3-11

**NACLC
NATIONAL AGENCY CHECK W/ LOCAL
AGENCY & CREDIT CHECKS**

- ◆ Military & Contractor personnel for Confidential and Secret Clearances
- ◆ Military Accessions for Air Force & Navy
- ◆ Commission an Officer in the Armed Forces
- ◆ Appoint a Warrant Officer, Cadet, Midshipman or Reserve Officer Training Candidate in the Armed forces
- ◆ Nuclear PRP Controlled Positions
- ◆ NATO Confidential and Secret
- ◆ ADP II Positions
- ◆ Interim Top Secret Clearance, if the other requirements have been satisfied

Figure 3-12

SSBI SINGLE SCOPE BACKGROUND INVESTIGATION

- ◆ Appointment to Critical Sensitive duties and Critical Sensitive positions
- ◆ Presidential Support Duties, Category I and II
- ◆ Nuclear PRP Critical positions
- ◆ ADP I positions and duties
- ◆ Limited Access Authorizations (LAAs)
- ◆ NATO Cosmic
- ◆ Access to Sensitive Compartmented Information (SCI)
- ◆ Access to Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI)
- ◆ Other Special Access Programs (SAPs) with DUSD(P) approval
- ◆ Top Secret clearances for military members, civilians and contractors

Figure 3-13

PR

PERIODIC REINVESTIGATION

- ◆ Conducted at 5-year intervals, except with DUSD(P) approval
- ◆ For Critical-Sensitive positions
- ◆ For Top Secret clearances
- ◆ For SCI
- ◆ For LAA
- ◆ For Presidential Support Duties
- ◆ For ADP I Positions
- ◆ For NATO Cosmic
- ◆ For some people accessing very sensitive information classified Secret

Figure 3-14

SII SPECIAL INVESTIGATION INQUIRY

- ◆ To prove or disprove allegations relating to the security criteria
- ◆ To assess the current eligibility of an individual previously adjudicated unfavorably if the potential need for clearance exists and there is reason to believe that the cause of the adverse determination no longer exists

Figure 3-15

OTHER PSIs

DSS and OPM are only two of the Federal agencies which conduct Personnel Security Investigations. Other PSI agencies include the FBI, CIA, NSA, State Department and the Coast Guard.

Generally speaking, a PSI conducted by one Federal agency may meet the requirements of any other Federal agency. All SSBIs, regardless of who conducts them, meet the same minimum requirements and therefore are reciprocal. This means that DSS will not conduct an SSBI on a DoD affiliated person if there's a current, valid SSBI conducted by another agency that meets the requirement of the position. The existing investigation may suit DoD's needs.

An SSBI conducted by one Federal agency must be accepted by other Federal agencies.

In addition to the SSBI, there are other investigations conducted for other Federal Agencies' PSPs. The most common of these are the Minimum Background Investigation (MBI) and Limited Background Investigation (LBI). Both of these investigations are conducted by OPM as part of the suitability and security programs of other Federal Agencies. Though these PSIs are not specifically used in the DoD PSP, sometimes they can be accepted in place of new investigations.

PSI EQUIVALENTS		
LBI	=	ENTNAC, NAC, NACI, ANACI, NACL
MBI	=	ENTNAC, NAC, ANACI NACL
BI	=	ENTNAC, NAC, ANACI NACL
SBI	=	SSBI

Figure 3-16

Finally, there are many PSIs on file which are still valid and current, but no longer meet the requirements of the regulation. The most common of these are the Background Investigation (BI) and Special Background Investigation (SBI). Both the BI and the SBI have been replaced by the SSBI. The SBI, which is also known as the Full Field Special Background Investigation (FF/SBI) and the BI (a.k.a. FF/BI), are no longer conducted by any Federal agency. Existing SBIs and BIs can sometimes be used instead of new investigations. Figure 3-16 shows the equivalency between these PSIs and those currently used in our program.

THE SCOPE OF PSIs

Each PSI used in the DOD PSP has certain minimum investigative requirements which must be met for the investigation to be considered complete. This is known as the "scope" of the investigation. It's critical for you to be aware of the scope of PSIs in order to properly adjudicate them. You need to know what constitutes a given type of PSI in order to know if the investigative agency has covered all the bases. Knowing the scope of an investigation also tells you what type of information you can expect from that investigation.

If you know the scope of a PSI, you know what to expect from it.

For instance, if you know the scope of an ANACI, you won't expect it to give you any neighborhood coverage, since that's not a part of an ANACI. On the other hand, when you review an SSBI, you know that you can expect it since it is routinely part of the SSBI.

Whenever you review a PSI, you will be "scoping" it, or making sure that it meets minimum requirements. Your CAF may require that you do it formally, with some sort of scoping aid, or you may be allowed to do it mentally as you're reviewing the case. In either case, you always scope an investigation to assure yourself that it is complete. We will only be discussing the scoping requirements of PSIs in this course. If you attend the resident phase of this course it will address how to scope out investigations, and what to do about PSIs which do not meet scope.

Scope refers only to the minimum investigative requirements.

The minimum investigative requirements for each type of PSI are shown in Figures 3-17 through 3-26 below. It's important to remember these represent the minimum requirements for each PSI. The investigative agency is free to obtain additional information when it chooses, and it will usually expand the investigation to resolve any issues raised.

This section contains only the major scoping elements; more detailed scoping information is found in the Nov 98 Memo (attachment 2). The scoping requirements of the

ANACI are shown in greater detail since the Nov 98 Memo does not address the ANACI scope.

NATIONAL AGENCY CHECK (NAC)

A NAC is a record check of certain Federal agencies. Only those agencies which maintain records containing information relevant to making a personnel security determination are checked. A NAC is also an integral part of each SSBI, PR, ANACI and NACL. Figure 3-17 shows the investigative elements of a NAC. Whenever one of the agencies checked has information on the subject, a copy is attached to the NAC results. When necessary, DSS will conduct additional investigation to resolve issues raised by the NAC. This is known as an ENAC or Expanded NAC. The ENAC is not a separate PSI.

ENTRANCE NATIONAL AGENCY CHECK (ENTNAC)

The ENTNAC uses a name check rather than a tech check at FBI/ID.

An ENTNAC is a variation of the NAC. The only difference is that the check at FBI/ID consists of a "name check only," rather than a detailed technical fingerprint search. This means that rather than run the subject's fingerprints through the FBI files (a "tech check"), they only run his or her name. This is done because given the typical age of first-term enlistees, a tech check is usually not productive - the subject just hasn't had much chance to be arrested. Those who have been arrested will usually be caught by the name check.

NATIONAL AGENCY CHECK W/LOCAL AGENCY AND CREDIT CHECKS (NACL)

A NACL is also a variation of the NAC. The only difference is that it contains a Credit Check and a Local Agency Check as part of the investigative scope.

ELEMENTS OF THE NAC

These agencies are always checked:

- ◆ DCII
- ◆ FBI/HQ (Investigative files of the FBI)
- ◆ FBI/ID (The Fingerprint Check)

These agencies are checked when the conditions shown in App. B, 5200.2-R are met:

- ◆ OPM SII
- ◆ INS
- ◆ State Department
- ◆ CIA
- ◆ Military Personnel Records
- ◆ Treasury Department
- ◆ The files of other agencies will be checked when pertinent.

Figure 3-17

OPM PSI

National Agency Check with Written Inquiries (NACI)

Access National Agency Check with Written Inquiries (ANACI)



Figure 3-18

The ANACI is conducted by written inquiry and includes no field investigation.

The NACI/ANACI is conducted by OPM using written inquiries. The period of investigation is the last five years of the subject's life. In addition to the valid NAC, the elements shown below represent minimum investigative scope. These are summarized in Figure 3-19.

EMPLOYMENT OPM will verify, by written inquiry, all employment in the last five years, regardless of duration. In addition, OPM will send a written inquiry about any involuntary termination, regardless of when it occurred.

EMPLOYMENT REFERENCE

COVERAGE. OPM will send a written inquiry to the listed supervisor of each employment for the last five years.

EDUCATION. All attendance at colleges and universities for the last five years will be verified by written inquiry. Additionally, OPM will verify all claimed degrees for the last 20 years.

LISTED CHARACTER REFERENCES.

Written inquiries are sent to all listed references.

LOCAL AGENCY CHECKS (LACS).

Written inquiries will be sent to law enforcement agencies at all places of employment, residence and education for the last five years. Additional inquiries will be sent to obtain the dispositions of all arrests developed, regardless of when they occurred.

CREDIT CHECKS.

OPM will schedule checks of credit bureaus any place subject has lived, worked, or gone to school for the last five years. The ANACI will contain copies of all credit reports which were obtained.

Additional investigation will be conducted as necessary to resolve any ***employment suitability*** issues which are raised by the ANACI. **OPM will not usually resolve security issues.**

ELEMENTS OF THE ANACI/NACI

- ◆ **Last Five Years**
- ◆ **NAC**
- ◆ **Employment Records**
- ◆ **Supervisors**
- ◆ **Education Records**
- ◆ **Listed Character References**
- ◆ **LACs**
- ◆ **Credit Checks**

Figure 3-19

SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)

***The SSBI
has a
10-year scope***

The period of investigation is the last ten years of the subject's life or back to the 18th birthday whichever is shorter. In any case, the investigation will cover at least two full years of the subject's life, but no investigation will be conducted before the 16th birthday. (This means that a subject must be at least 18 years old to have an SSBI.) Figure 3-20 shows the major elements of the SSBI. In addition to those shown, DSS will conduct any investigative leads necessary to resolve issues raised by the SSBI.

ELEMENTS OF THE SSBI

- ◆ Last 10 years
- ◆ NAC
- ◆ Spouse NAC
- ◆ Subject Interview
- ◆ Employment Records
- ◆ Employment Interviews
- ◆ Military Service and Discharge Verified
- ◆ Developed Character References
- ◆ Listed Character Reference
- ◆ Neighborhood Interviews
- ◆ Local Agency Checks
- ◆ Credit Checks
- ◆ Ex-Spouse Interview

Figure 3-20

PERIODIC REINVESTIGATION (PR)

The purpose of the PR is to up-date the SSBI. Its period of investigation is the last five years of subject's life. Figure 3-21 shows the major elements of the PR. In addition, the PR will be expanded to explore all leads necessary to resolve any issues raised in the course of the PR.

ELEMENTS OF THE PR

- ◆ Last 5 years
- ◆ NAC
- ◆ Spouse NAC (if we don't have on file)
- ◆ Subject Interview
- ◆ Employment Records
- ◆ Employment Interviews
- ◆ Developed Character References
- ◆ Neighborhood Inquiries
- ◆ Local Agency Checks
- ◆ Credit Checks

Figure 3-21

SECRET PRs

Secret PRs are conducted for personnel who have Secret level access, not just a Secret clearance with Confidential or no classified access.

Secret PRs

- * Secret level SAPS
- * Secret clearance/access
- * Due every ten years
- * Exceptions
 - Current derogatory information
 - Saps

A cartoon character with a yellow face, wearing a blue suit and red tie, is shown from the chest up. He has a speech bubble above him that says "Checking on my clearance?".

04/02/96 45

Figure 3-23

Confidential PRs

- * Confidential clearance/access
- * Due every fifteen years
- * Exceptions
 - Current derogatory information

A cartoon character with a yellow face, wearing a blue suit and red tie, is shown from the chest up. He has a speech bubble above him that says "Checking on my clearance?".

04/02/96 45

SPECIAL INVESTIGATIVE INQUIRY(SII)

The SII is an issue-resolution investigation. That means there are no minimum investigative requirements for an SII. The SII is scoped to cover all leads necessary to resolve the outstanding issues after the initial Personnel Security Investigations has been conducted and adjudicated.

OTHER PSIs

A PSI from a non-DoD agency is acceptable if meets scope

In addition to the PSIs conducted as part of the DoD PSP, investigations are conducted for other federal agency PSPs. These investigations "shall be mutually and reciprocally accepted by all agencies", IAW EO 12968, Sec.2.4, as meeting the requirements of the DoD PSP, unless an agency has substantial information indicating that an employee may not satisfy the standards in Section 3.1 of the EO.

An SSBI conducted by any Federal agency will meet the same scope as a DSS SSBI and shall be accepted by DoD agencies.

The MBI (Minimum Background Investigation) and the LBI (Limited Background Investigation) are conducted by OPM and have no counterparts in the DoD PSP. They can be considered the equivalent of the ANACI, NACLIC, NAC and ENTNAC, and can take the place of any one of them. The investigative elements of the MBI and the LBI are shown below in Figures 3-24 and 3-25, respectively.

ELEMENTS OF THE MBI

- ◆ NACI
- ◆ Credit check
- ◆ Telephone follow-up on written inquiries not returned.

Figure 3-24

ELEMENTS OF THE LBI

- ◆ NAC
- ◆ Subject interview
- ◆ Interviews of selected sources for the last 1-3 years
- ◆ Written inquiries and record searches for the last 5 years
- ◆ Credit Checks

Figure 3-25

Besides these investigations, there are two others you're likely to run across. These are the Special Background Investigation (SBI) and the Background Investigation (BI). Although these PSIs are no longer conducted by any Federal agency, there are still many valid BIs and SBIs on file.

The SBI is the equivalent of the SSBI. Although there are a number of differences between them (for instance the SBI covered 15 years rather than 7), a current, valid SBI will meet the scoping requirements of the SSBI (see Figure 3-20) and can take its place.

The old BI used to be the standard PSI used to grant Top Secret clearances and eligibility to perform critical sensitive duties. Figure 3-26 shows the scoping elements of the BI.

ELEMENTS OF THE BI

- ◆ Last five years
- ◆ NAC
- ◆ Subject Interview
- ◆ Employment Records
- ◆ Employment Interviews
- ◆ Developed Character References
- ◆ Local Agency Checks
- ◆ Credit Checks
- ◆ Subject Interviews

Figure 3-26

THE SUBJECT INTERVIEW

As you saw in the section on the scope of PSIs, the subject interview is an integral part of some PSIs and is occasionally found in most of the other PSIs. The SSBI and PR routinely contain subject interviews and the NACLC, NAC and SII contain them whenever there are issues to be resolved. In fact, the only PSI you'll deal with that never contains a subject interview is the ANACI. Even the ENTNAC may contain one if the subject is being submitted for a clearance and unresolved issues are present.

So why is the subject interview so important? The main reason is that the subject is the most knowledgeable source available. Nobody knows as much about the subject as the subject him/herself.

The subject knows more about himself than anyone else.

All other sources are secondary to the subject in terms of how much they know, so it only makes sense to use the subject as a source. (Of course, we can't consider him/her to be a *disinterested* source of information, so the investigation will always include other sources - just to make sure that the subject told "the truth, the whole truth and nothing but the truth"). This approach is also in keeping with the Privacy Act of 1974 which provides that, to the extent possible, information should be obtained directly from the individual concerned rather than from other sources.

When the subject interview is a routine part of the investigation, as in the SSBI and PR, it's called the SSBI SI. It is a wide ranging interview covering a number of topics. The subject is asked to verify the information on the SSBI.

When the subject interview is used to resolve issues which are developed in the course of the investigation, it's called the Issue SI. This latter function of the subject interview, issue resolution, is the reason subject interviews are conducted in the SII, NACLIC and NAC and sometimes the ENTNAC. The subject interview in these cases is always issue-oriented and answers questions which the investigation has raised. This sort of subject interview may deal with any of the security criteria and adjudication guidelines which will be discussed later in this lesson.

MID-WAY SUMMARY

We have begun our discussion of PSIs. We have looked at the types of PSIs used in the DoD PSP. You have learned that each PSI is different from each other PSI, and is used for different personnel categories. In addition, you have learned the clearance and sensitive duty levels authorized by each PSI.

We have also looked at the minimum investigative requirements (scope) of each PSI. You have learned that PSIs range from the NAC, which is just a computer check, to the SSBI, which is an extensive seven-year check of subject's background. You have learned some general scoping rules for DSS PSIs, as well as the specific requirements for each PSI.

Finally, you have learned about the two types of subject interviews, those routinely conducted to meet scope (the SSBI SI) and those conducted for issue resolution (the Issue SI). Now we will look at the investigative forms used with each PSI.

INVESTIGATIVE FORMS

"An investigative form is any official form or document which reports investigative information or results."

Besides the PSI request forms we discussed earlier, there are a number of other investigative forms with which you must be familiar. Just as each type of PSI has its own request forms, so also each has its own investigative forms. For our purposes, an investigative form is any official form or document which reports investigative information or investigative results. Investigative forms include the PSI request forms because they contain so much information about the subject. They also include the various forms used by DSS and OPM to report the results of their investigations. Samples of the most common investigative forms are included in the Investigative Forms packet.

Now, we will only look at the different types of forms, their uses, and how to review these forms. The PSIs of which they are part will be taught in the resident phase of this course.

NATIONAL AGENCY CHECK (NAC)

Besides the SF 86, the primary form used in reporting NAC results is the DSS Form 1. (These forms are listed in Figure 3-27.) The DSS Form 1 is the standard form used by DSS when reporting the results of an investigation. When used for a NAC, it is known as a Report of NAC, or RON.

A sample of a DSS Form 1 completed with favorable NAC results is shown in the reading packet. As you can see, DSS reports the agencies contacted and the results of the contact. When there is information reported by one of the agencies contacted, it is attached to the RON. Such information could include prior investigations, an FBI arrest record (a "rap sheet") or information from subject's military record.

NAC FORMS

- ◆ SF-86 (Questionnaire for National Security Positions)
- ◆ DSS Form 1 (Report of NAC)
- ◆ Additional information may be attached

Figure 3-27

ACCESS NATIONAL AGENCY CHECK WITH WRITTEN INQUIRIES (ANACI)

Because it is conducted by written inquiry, the ANACI has a wide range of forms which are routinely used to report investigative information, as stated in Figure 3-28. The SF 171 or equivalent, the SF 85, SF 85P, SF85-PS, and SF 86 all contain a great deal of information provided by subject and are used by OPM as source material for sending written inquiries (known as "vouchers") to the subject's former employers, etc.

You're familiar with the old SF 171, the Application for Federal Employment. The most important information on this form is on the last page. Pay close attention to Subject's responses to those questions.

The SF 85 is the Questionnaire for Non-Sensitive Positions. This is the form used when the Subject has no clearance and performs only non-sensitive duties.

If Subject is assigned to a Non-DoD agency performing duties in a Non-Critical Sensitive duties, but has no access to classified information, the SF 85P (Questionnaire for Public

Trust Positions) is used. Questions 15 through 21 are especially important.

The application form you'll see most often is the Questionnaire for National Security Positions, the SF 86. DoD agencies use this form to request ANACIs for Secret and Confidential clearances and assignment to Non-Critical Sensitive positions.

The OFI prefix on vouchers stands for the Office of Federal Investigations.

When reviewing this form pay close attention to Part 2 of the source's answers to specific questions. Each form also includes a "Remarks" section for the source to say whatever he or she wants.

NACI/ANACI FORMS	
SF 171	Application for Federal Employment
SF 85	Questionnaire for Non-Sensitive Positions
SF 85P	Questionnaire for Public Trust Positions
SF 85PS	Supplemental Questionnaire for Selected Positions
SF 86	Questionnaire for Sensitive Positions
OFI 41	Investigative Request for employment Data and Supervisory Information
OFI 42	Investigative Request for Personal Information
OFI 43	Investigative Request for Educational Registrar and Dean of Students Record Data
OFI 44	Investigative Request for Law Enforcement Data
1-4e	FBI ID Division Rap Sheet

Figure 3-28

OFI 40

The OFI 40 is known as the General Request for Investigative Information. It is the only non-specific voucher used by OPM. Because of this, it's used in a variety of situations whenever one of the specific vouchers isn't suitable. Probably its most common uses are to verify military service and to get Immigration and Naturalization Service (INS) records.

OFI 41

The OFI 41 is the Investigative Request for Employment Data and Supervisor Information. An OFI 41 is sent to the personnel office of every employer listed on the SF 171 and SF 86, 85P or 85 for the last five years. In addition, one is also sent to every listed supervisor for the same period.

OFI 42

The OFI 42 is the Investigative Request for Personal Information. It is sent to each reference listed on the investigative forms.

OFI 43

The OFI 43 is the Investigative Request for Educational Registrar and Dean of Students Record Data. This form is sent to each college or university subject has attended within the period of investigation (POI). It is also used to verify any claimed degrees regardless of whether they were earned in the POI.

OFI 44

The last voucher is the OFI 44, the Investigative Request for Law Enforcement Data. This form is sent to the Police Department or Sheriff's Office wherever subject has lived, worked or gone to school within the POI. It may also be sent to courts to obtain the disposition of an arrest.

Finally, the 44 is used to **verify** any arrest or conviction listed on the investigative forms regardless of when it occurred.

The 1-4e is the FBI rap sheet.

The next most common form used in ANACIs/NACIs is the 1-4e - the FBI "rap sheet". The rap sheet records the results of the FBI/ID "tech check" - the fingerprint check. The rap sheet is a listing of all arrests recorded under subject's fingerprints, as shown in the National Crime Information Center (NCIC), which is maintained by the FBI. The date and place of arrest are shown and, when

available, the disposition (conviction, etc.) is listed.

It's important to realize that the only arrests shown on the rap sheet are those reported to the FBI. The subject may have dozens of other arrests which, for one reason or another, aren't reported to the NCIC. With luck, the LACs will catch those.

When fingerprints are unclassifiable, the tech check is done by name check only.

Occasionally the subject's fingerprints are unclassifiable which means they can't be "read" and matched with prints on file. In this case, the FBI does a name check and makes up a rap sheet of all arrests listed under the subject's name - even if they aren't the subject's arrests. This means that frequently arrests are incorrectly ascribed to the subject because of his/her name - you can imagine the problem someone named "John Smith" might have. Clearly these records need to be checked closely to be sure that you don't hold the subject responsible for someone else's actions. When

the tech check is done by name, the top of the rap sheet will say "Name Check Only."

In addition to these standard or routine forms, any number of other forms may be sent in by sources. These include employment forms, state and local police rap sheets and general correspondence. It is impossible to predict when any of these other forms may appear in a NACI, but they all require close attention when they do.

SSBI, NACLCL, NAC, ENTNAC, PR AND SII

The SSBI, NACLCL, NAC, ENTNAC, PR and SII all use the same forms (see Figure 3-29). The SSBI, NACLCL, ENTNAC, PR and SII contain a SF 86 on the subject and certain relatives of the subject (see "Scope of PSIs", page 30 of this lesson). The SF 86 is a rich sources of information on the subject. The NAC contain the SF-85P. In addition to these forms, DSS uses a number of others to report investigative results in these PSIs.

The DSS Form 1 is the major form used in the SSBI, NAC, NACLCL, ENTNAC, PR and SII.

The most common form used in these investigations is the DSS Form 1, the Report of Investigation (ROI). The DSS Form 1 is used to report the vast majority of investigative results, including the results of interviews and record checks. A copy of an ROI reporting results is shown in the Investigation Forms Packet.

Whenever subject provides a signed statement, DSS uses two forms - the DSS Form 23a and the DSS Form 24. The 23a is used as the first page of the subject statement. It contains the Privacy Act.

SSBI, PR AND SII

DD Form 1879	Request for Personnel Security Investigation
SF 86	Questionnaire for National Security Positions
DSS Form 1	Report of Investigation) (ROI)
DSS Form 23a	Statement (first page)
DSS Form 23a	Statement of Subject (first page)
DSS Form 24	Statement Continuation Sheet (signature page)
Credit Report	CBM standard credit reporting form
PIC Form 13	Notice from PIC

Figure 3-29

A signed statement from a subject is given on DSS Forms 23a and 24.

Advisement and a notice that the statement is voluntary. The final page of the statement is the DSS Form 24, which has places for the subject, the Special Agent and two witnesses to sign their names (you'll almost never see witness signatures). If additional pages are required,

regular typing paper is used and inserted between the 23a and the 24.

A signed statement from a source goes on DSS Forms 23 and 24.

When DSS obtains a signed sworn statement from a source other than subject, the DSS Form 23 is used. This form differs from the Form 23a in that it lacks the Privacy Act Advisement. Otherwise, a source statement is reported in the same way as a subject statement (that is with the Form 24 and typing paper).

The DSS Form 154 is used when the subject has financial problems.

When DSS interviews the subject about his/her financial situation, the Special Agent will often have the subject provide a Personal Financial Statement, DSS Form 154. The 154, which can run to more than one page if necessary, lists the subject's monthly income, monthly expenses, debts, monthly debt payments and assets. It contains a great deal of information and requires close review. The 154 will always be accompanied by a Subject's statement (on DSS Forms 23a and 24).

When the DSS investigation includes a credit report, it is reported in one of two ways. A favorable report is reported on the DSS Form 1 with the following statement: "A review of credit bureau records at the following locations disclosed no unfavorable information."

Unfavorable or negative credit information is reported by the DSS vendor using a common report format. This form contains Subject's name, address and other personal identification data (PID). It also lists the subject's creditors and the status of each account. The back of the form contains a key to any codes used in the credit report. (This subject will be discussed later in this lesson under the block entitled, "The Credit Report".)

The PIC Form 13 provides information about the investigative process.

The final form regularly found in these investigations is the PIC Form 13. This form is used by the Personnel Investigations Center (PIC) to communicate with the CAF or the requester of the investigation. The PIC may notify you that investigative coverage of a particular activity was not possible and why. Or the PIC may include a microfiche copy of a prior investigation which was conducted on the subject. Any information conveyed by the PIC Form 13 will refer to the investigative process rather than the investigative results, but nevertheless can be very important in reaching an adjudicative determination.

COMMON PROBLEMS WITH PSIs

Now we'll conclude our discussion of PSIs. We just finished looking at the types, uses, scope of PSIs and the investigative forms found in each PSI. Now you'll learn about some of the most common errors and problems found in completed PSIs.

You need to be aware of these problems when you review PSIs. We will only introduce you to the problems and errors, and help you to identify them. Resolution of these issues will be taught in the resident phase of this course.

One of the major problems with conducting and reviewing PSIs is the number of errors found in PSI request packages. These errors range from incomplete information on the request forms to deliberate attempts by the subject to deceive. Figure 3-30 shows the most common errors.

COMMON ERRORS

- **Incomplete Information**
- **Discrepant Information**
- **Deliberate Falsification**

Figure 3-30

The most common error in PSIs is incomplete info from the subject.

The most common error is incomplete information on the personnel security questionnaires - the SF 85, 85P and 86. The subject frequently provides only partial information when answering the questions on these forms. For instance,, Question 21 of the SF 86 asks, **"In the last 7 years, have you consulted with a mental health professional (psychiatrist, psychologist, counselor, etc.), or have you consulted with another health care provider about**

a mental health related condition?" A "yes" answer must be explained. If the subject answers "yes" but fails to fully explain his/her answer, it could cause DSS to reject the investigation request.

You must be aware of incomplete info and decide how to resolve it.

There's also the possibility that the investigative agency won't reject the case, but won't resolve the issue either. It's your responsibility as an adjudicator to be aware of the incomplete information and determine if additional investigation is needed to resolve the issue.

Such mistakes can be accidental (due to carelessness) or deliberate (due to an attempt to deceive). It's not unusual for the subject to provide partial information on purpose, hoping that no one will notice. When the investigator comes knocking on the door for more information, the subject can simply plead that it was an oversight or that he/she misunderstood the question.

It may also be due to the subject's belief that the information asked for is none of the government's business. Given the personal nature of many of the questions we ask, this isn't really a surprising reaction. Regardless of the cause, the result is the same: you must be thorough in your review of investigative forms to make sure that you have all the information you need to make a decision.

Another common error in PSI packages is contradictory information provided by the subject. This is most common in ANACIs/NACIs because they always have two forms giving similar information - both the 171 and the 85, 85P or 86.

You'll find that it's not uncommon for the subject to list a different employment history on the 171 and the 85, 85P or 86. This also may be deliberate or accidental. Frequently, the subject fills out the forms at different times without any reference material (such as a resume). In such a case, discrepancies are almost unavoidable.

Request forms frequently contain

It's important that you be aware of any discrepancies because of what they may conceal, such as a firing or even imprisonment. Though this problem is more common with the NACI, you'll also find it with other PSIs. For instance on the 86, the subject may show that he/she was

discrepant info.

simultaneously living and working in geographically remote areas. Although this may have a simple explanation, it may also conceal something pertinent to your adjudication.

The final common "error" in PSI packages is the deliberate lie. Sometimes this will seem like the most common error of all, and it does happen frequently. The subject seems to have the theory that "What I don't say can't hurt me" and lies about his/her arrest record, drug and alcohol history, credit status, etc.

Subjects may lie on their forms.

A deliberate lie on one of the investigative forms will only be revealed, if at all, by the investigation - when the rap sheet, credit report, etc., come in. There is no way of telling how often deliberate lies go undiscovered. This situation shows that while the subject may be the most knowledgeable source, he/she isn't necessarily the most reliable.

All of these errors require close review of the PSI packages, both to prevent rejection by the investigative agency and to ensure proper adjudication. Although you can't prevent these errors, by careful review you can reduce their damage.

COMMON PROBLEMS WITH PSIs

Besides the errors that the subject makes when filling out the investigative forms, there are a number of other problems with the various PSIs used in the DoD PSP. Understanding these problems will help you to make better informed decisions when adjudicating PSIs.

THE NAC & ENTNAC

The NAC doesn't develop new information.

The NAC and ENTNAC are the PSIs with the most severe problems. The major problem is with the scope of these investigations. They are not designed to develop information, but rather to consolidate existing information. It only taps existing federal record banks and consolidates the information found into a single report. Many of the richest sources of information about the subject (e.g. LACs, employment and reference checks, credit reports) are never checked or reported. Although the subject is asked to provide a great deal of information, there is no way of verifying the information or determining the truthfulness of the subject without any field investigation. As a part of another investigation, like the SSBI, ANACI, NACI or NACLCL, the NAC and ENTNAC are enormously useful. As a stand alone investigation, their utility is severely limited

THE NACLCL

The NACLCL, although a broader investigation than the NAC or the ENTNAC, it too has a few problems. Although the NACLCL includes a check of the Local Agencies and Credit Bureau, it lacks sources of information about the subject (e.g. employment and reference checks. As in the case of the NAC and ENTNAC, subject is asked to provide a great deal of information; however, there is no way of verifying the information or determining the truthfulness of the subject without any field investigation. However, if those checks covered in the NACLCL disclose questionable or derogatory information, the investigation will be expanded in attempts to resolve such information.

THE ANACI

The ANACI and NACI is a vastly better investigation than the NAC, ENTNAC or NACLC, but it has a number of severe problems. These problems are shown in Figure 3-31 and discussed below.

PROBLEMS WITH ANACI AND NACI

- ◆ Primarily an employment investigation (NACI only)
- ◆ No field investigation conducted
- ◆ No context for sources' comments
- ◆ Failure to resolve issues
- ◆ The subject "controls" the investigation

Figure 3-31

Although DoD uses the ANACI as an investigation for determining eligibility for a security clearance and/or eligibility to perform sensitive duties, the ANACI also is designed to be an employment suitability investigation for assignment to non-critical sensitive positions. The NACI is used within DoD as an employment suitability investigation for assignment to non-sensitive positions.

As a matter of fact, non-DoD Federal agencies don't even use the ANACI. They use the NACI only for employment considerations.

The ANACI and NACI focus places limits on the amount and type of information you have to adjudicate. It also means that the ANACI and NACI are better at raising questions than answering them. When reviewing

The ANACI & NACI are better at raising questions than answering them.

A derogatory ANACI or NACI, you'll frequently find that you have questions about the subject's security suitability, but no answers.

The reason that there are no answers is that OPM will not expand an ANACI or a NACI to resolve security questions, only employment suitability issues. If there are security suitability issues to resolve, the requester must either pay OPM to re-open the case or turn to another agency, such as DSS to conduct a SII.

The NACI & ANACI are conducted thru the mail.

The second major problem with the ANACI and NACI are the way they are conducted. They involve no field investigation: no investigator interviews the sources or checks the records involved. OPM sends vouchers by mail to the various sources. From the point of view of a source, these vouchers are unsolicited mail, sometimes "junk mail".

You can guess at the fate of a voucher viewed as junk mail - all too often it ends up in the wastebasket. Even when that doesn't happen, it may be weeks or months before the source gets around to filling out the voucher, which may be a low priority item from his or her point of view. To further complicate matters, the vouchers have to be filled out with a #2 pencil, since they're machine readable. If the source doesn't happen to have any #2 pencils, he may decide to just throw the voucher away.

If the vouchers aren't returned, OPM will usually simply close the ANACI or NACI, calling it a completed investigation. This is true even when the majority of the vouchers aren't returned. When that happens, you must simply adjudicate what you have. You would not normally re-open or expand the case unless you had a specific reason to do so.

When the vouchers are filled out and returned, there are still problems. Because there is no field investigation, there's no opportunity to have the sources explain their comments, to provide background and context for their replies. For instance, when a source says: "The only problem with Joe is that he drinks too much", the statement is almost meaningless without further

information.

In fact, it may say more about the source than about the Subject. "Too much" is a relative term which can mean significantly different things depending on whether the source is a tee-toteler, a social drinker, or an alcohol abuser. The point is, such a statement raises questions but fails to answer them. If the ANACI or NACI too often fails to answer questions, at least it does ask them. As long as an issue is raised, you can get additional investigation to resolve it and answer the questions. An SII from DSS is often needed to resolve issues raised in an ANACI or NACI before you can make a final adjudication. So although issue resolution is a major weakness of these investigations, issue identification is one of its major strengths.

The next problem with the ANACI and NACI is related to those already mentioned. Because no field work is conducted, the subject controls the investigation. That is, he or she provides the only lead information. Vouchers are only sent to those employers, schools, reference and police departments that the subject shows on the SF 171 and SF86. As you've already learned, it's not unusual for a subject to lie on these forms. This is a serious problem because the ANACI and NACI provide no opportunity for the investigation beyond the subject's control, to inquire about those areas of life that the subject may choose to conceal.

For instance, if the subject was terminated from an employment because of embezzlement, you probably won't know about it if he/she fails to list that employment on the SF 171 or 86. If, however, an investigator was in the field, asking questions and reviewing records, the information would probably be developed.

THE SSBI AND PR

The answer to the NAC, ENTNAC, NACL, ANACI and NACI problems we've discussed is the SSBI and PR. All of the problems brought up in the other investigations are solved here. SSBIs and PRs, being field investigations, are able to develop new sources of information about the subject (such as employment and neighborhood references), as well as tap existing sources (such as national agencies and credit bureaus). These investigations are designed to determine security suitability, although they are also used for employment suitability. All in all, these investigations are the most complete and the most satisfying to deal with. They are not, however, perfect. A number of problems are shown in Figure 3-32, and discussed below.

COMMON PROBLEMS WITH SSBIs AND PRs

- **Sometimes fail to resolve issues**
- **Abbreviated Report Format**

Figure 3-32

It's a truism, but one worth keeping in mind: An investigation is only as good as the investigator who runs it. This is especially true in the SSBI and PR.

"An investigation is only as good as the investigator who runs it."

While these investigations usually resolve all issues Raised, they occasionally leave unanswered questions. Sometimes a Special Agent will fail to resolve an issue or fail to pursue logical areas of follow-up. When that happens, you may need to re-open the case to get additional information.

It's also a truism that adjudicators always want more information, regardless of how much they already have. These investigations wet this appetite for more information, but don't satisfy it.

"Abbreviated Report Format" shows contact but not substance of comments.

They are usually reported in the "Abbreviated Report Format". In this format the contact with a source is reported, but the substance of the source's comments are only reported if there is something discrepant or derogatory. As an adjudicator, you have to take it on faith that the investigator covered all of the necessary bases. Figure 3-33 shows the general areas of questioning which are *always* covered in each of these contacts.

GENERAL AREAS OF QUESTIONING IN A DSS INTERVIEW

Nature, Period & Frequency of Association of Source & Subject

Subject's Reliability & Trustworthiness

Subject's Criminal Conduct & Moral Conduct

Subject's Use of Alcohol and Drugs (include. Marijuana)

Financial Responsibility

Any Foreign Travel & Connections

General Reputation of Subject, Family & Associates

Subject's Loyalty to the United States

Does Source Recommend Subject for a Clearance /Sensitive Duties

Any Collateral Verification of Activities

Figure 3-33

THE SPECIAL INVESTIGATIVE INQUIRY (SII)

It isn't really possible to discuss the SII in terms of common problems. The SII, being such a tightly focused, issue oriented investigation, can't be discussed in any meaningful way. Problems with SIIs tend to be individual rather than generic, as the problems are with an individual SII rather than with all SIIs.

THE CREDIT REPORT

Now we'll discuss the credit report, and the role it plays in adjudication. You'll learn when DSS and OPM obtain credit reports and when and why they provide them to you to adjudicate.

This information will help you to understand why the credit report is such a valuable tool and why it plays such a big role in adjudication.

ORIGIN OF CREDIT REPORTS

If you go to buy a car, rent an apartment, apply for a charge card, you expect to be the subject of a credit check - it's a routine part of doing business in this day and age.

Increasingly, it's also a routine part of the business of personnel security. All applicants for security clearances or sensitive duties will also be the subject of credit checks.

This hasn't always been the case. Credit reports are a relatively recent invention in the business world, and even more of a newcomer to the world of personnel security.

The first credit bureau wasn't established until 19th century London tailors, fed up with being paid when and

if their customers saw fit, got together and pooled information on their customers' payment habits. Now they could be fairly confident about who would pay a bill promptly (a "good credit risk") and who should be asked to pay in advance (a "bad credit risk").

Needless to say, an idea that's good is going to catch on, and the growth of the credit reporting industry has been nothing short of explosive. In this country alone, there are about 1,400 different credit bureaus, all dedicated to separating the good credit risks from the bad. It's estimated that these bureaus maintain information on 80% of all American households.

Credit reports have only been part of the investigative and adjudicative process since about 1980. Since that time they've become an increasingly important part of the PSI, until now they're recognized as one of the most valuable tools available to us in personnel security.

WHY HAS THE CREDIT REPORT BECOME SO VALUABLE?

The main reason is the changing nature of the American spy. At one time, Americans became involved in espionage because of a variety of reasons - ideology, blackmail, etc. Now we do it for the money!

*Americans spy
because of
money.*

The sad truth is that most Americans who sell out their country, do it to make a buck.

This means that any source of information which tells us about a subject's financial habits (about how well the subject lives and how much he/she owes) is valuable. Anything which shows us a subject who is deeply in debt, or one who is living beyond his or her known means, may be showing us a subject who is a potential spy.

WHEN WILL YOU RECEIVE CREDIT REPORTS?

The credit report is such a valuable tool that it is part of every PSI conducted to determine eligibility for a security clearance and/or assignment to a sensitive position for the DoD PSP. In fact, all PSIs don't include a credit report. Figure 3-34 shows those which do.

PSIs CONTAINING CREDIT REPORTS

Credit Reports are routinely part of the:

- * **SSBI**
- * **PR (TS, S, and C)**
- * **ANACI**
- * **NACI**
- * **NACLC**

Credit Reports may be part of the:

- * **SII**

Figure 3-34

HOW DOES DSS CONDUCT CREDIT CHECKS?

When the PIC receives a DD 1879 and a SF-86 requesting an investigation, the first thing the case controller does is review them to decide what investigation needs to be done. This is called "scoping" the investigative leads. Also, the case controllers scope the credit leads.

The case controller marks each address where the subject has lived, worked, or gone to school for a total of six months or more (cumulatively) during the last seven years for an SSBI or the last five years for a NACLIC and PR. In addition, each name that subject has used, including maiden names, former married names and aliases, is also marked by the case controller. These are the credit leads. DSS will obtain credit checks at each place marked, under each name marked. So if six places are marked, and subject has a married and a maiden name, up to 12 (6 x 2) credit reports could be obtained.

THE CREDIT VENDOR

DSS doesn't actually go out and conduct the credit leads itself. It would be an enormous investigative burden, and a contractor can do the job more easily. Because of this, DSS has a contract with a national credit vendor, who conducts all the credit checks for DSS PSIs.

This vendor is not an actual credit bureau itself. Instead, it acts as the middleman between DSS and the national credit bureau systems from whom it gets credit reports. The vendor doesn't deal with all of the 1,400 credit bureaus in the U.S., because most of them are small, local operations, known as "mom and pop" credit bureaus.

Instead, the vendor deals only with three national credit bureau systems - the super powers in the world of credit reporting. Figure 3-35 shows the national credit bureaus.

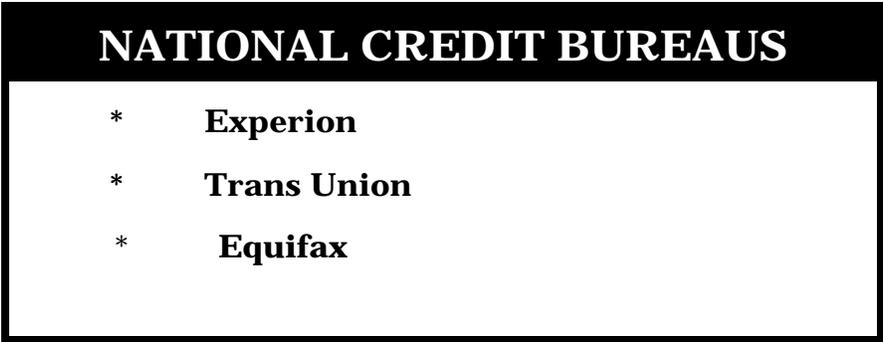


Figure 3-35

Each of these credit bureaus provides coverage for the entire United States. However, each bureau is not equally strong in each area. For instance, TRW might be strong in Washington, DC, but much less strong in El Paso, TX. CBI, on the other hand, may be strong in El Paso, but weak in DC. These various strengths and weaknesses of the different credit bureaus are recorded in what's called the

DSS uses the best credit bureau for each locale.

Customer Table. This is a listing, by zip code, of each locale in the United States, and the major credit bureau which provides the best coverage in that area. The credit vendor uses the Customer Table to decide which credit bureau to use.

That means that when DSS runs an SSBI on a subject, the credit vendor compares the credit leads to the Customer Table, and requests credit reports from the strongest credit bureau in each place subject has lived, worked or gone to school in the last seven years. For instance, a subject currently works in Washington, DC, but graduated from El Paso State College last year. The vendor will get a credit report from Experion for DC and one from Equifax for El Paso. This ensures that the best information is obtained at each place. OPM gets credit reports for the ANACI in essentially the same way.

HOW DOES DSS REPORT CREDIT INFORMATION?

When the vendor gets all the credit reports, it translates them into a common reporting format and forwards them to the PIC. The PIC case analyst reviews the credit reports and decides if they're derogatory or not (that is, if the bad debts total more than \$2000.00) or if further expansion is necessary. A detailed report describing the credit history is provided in all PSI's containing a credit check.

When the credit check contained unfavorable credit information, the case will contain a statement that the credit check disclosed unfavorable information as shown in Figure 3-36. This statement will appear prior to the credit report itself.

CREDIT

REVIEW OF CREDIT BUREAU RECORDS COVERING THE FOLLOWING LOCATIONS DISCLOSED UNFAVORABLE INFORMATION -

RICHMOND, VA
FOSTER, VA

Figure 3-36

When there are several credit checks in a case, it isn't unusual for some of them to be favorable, while others contain derogatory information. When that happens, the results are reported as shown in figure 3-37, with some of the credit reports provided to you and the others destroyed.

CREDIT

REVIEW OF CREDIT BUREAU RECORDS COVERING THE FOLLOWING LOCATIONS DISCLOSED NO UNFAVORABLE INFORMATION -

RICHMOND, VA
FOSTER, VA

CREDIT

REVIEW OF CREDIT BUREAU RECORDS COVERING THE FOLLOWING LOCATIONS DISCLOSED UNFAVORABLE INFORMATION - SEE ATTACHED

BOSTON, MA
MILTON, MA

Figure 3-37

In addition to preparing the ROI, the case analyst decides if the information needs to be resolved by a field investigation. If so, the case analyst scopes the necessary leads to the field, and an agent resolves any issues. Needless to say, your PSI will include the results of this investigation as well as the credit report.

The PSI, with the credit reports and/or the ROIs is then sent to the CAF by the PIC. Figure 3-38 shows this whole process.

FLOW OF CREDIT REPORTS

PIC/FIPC reviews the case papers, scopes the credit leads, and sends them to the vendor.



The vendor compares the leads to the Customer Table and sends them to the appropriate credit bureaus.



The credit bureaus (TRW, CBI and Trans Union) generate credit reports for each name shown and send the reports to the vendor.



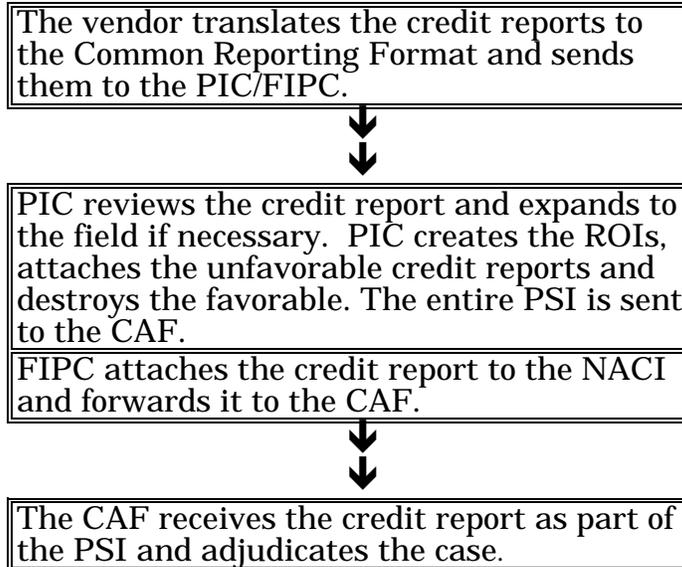


Figure 3-38

HOW DOES OPM REPORT CREDIT INFORMATION?

Unlike DSS, OPM always provides a copy of any credit reports it obtains. The credit report is attached after the NAC results and before any voucher responses. When the credit report contains derogatory information, OPM uses the same standard reporting format as DSS (see the "How to Read Credit Reports" booklet). Completely favorable reports use a different, more easily read format. A copy is at the end of the "How to Read Credit Reports" booklet.

OPM lists the results of the credit report check on the Case Closing Transmittal, which is the cover sheet for a complete ANACI. Figure 3-39 shows how the Case Closing Transmittal lists the results of three credit checks. The first one is a favorable credit report; the second is an unfavorable credit report; and the third one contained no pertinent information on the subject.

ITM ***	TYPEITEM IDENTIFICATION *****	CM **	RESULTS *****
E01	CREDEL PASO, TX	I	ATTACHED
E02	CREDBOSTON, MA	I	ISSUE
E03	CREDWASHINGTON, DC	I	NPI

Figure 3-39

WHAT INFORMATION IS IN THE CREDIT REPORT?

The credit report can be a rich source of useful information, if you keep a couple of things in mind.

The first is that the credit report was not designed with you, the adjudicator, in mind. It was designed to help creditors decide if someone is a good credit risk. It can help you decide if subject is a good security risk, but remember that's not what it's for. There's a world of difference between a *good credit risk* and a *good security risk*. Because of this, you'll find the credit report is full of information that seems useless to you but which is vital to credit grantors. On the other hand, it won't have some pretty obvious things that you need and think it should contain, but which creditors don't need or want.

The second thing to remember is that the credit report is not infallible. That old saying about computers - "garbage in, garbage out" - is even more true of credit reports. It's not unusual for a credit report to be full of bad (incorrect) information. If the creditors report something to the credit bureau, the credit bureau will presume it's accurate and repeat it to you. Only on closer examination will it be clear that it's all a mistake, misunderstanding, etc. All of this means that you have to be careful not to take the credit report at face value. In other words, treat it like any other source of information - hopefully, but not necessarily, accurate.

With this in mind, there's a lot you can get from a credit

Credit reports often contain incorrect information.

report. It can verify subject's residential and employment history. More than once a credit report has revealed a previously undisclosed spouse. Most of the time though, a credit report will reveal two types of information.

Delinquent debts may indicate trouble.

The first type deals with bad debts. A credit report will tell you when your subject is teetering on the edge of financial disaster. The credit report will identify the subject who's being dunned by bill collectors, or ending up in court for non-payment of debts. This information is critically important because a subject in financial trouble may turn to espionage to raise money. Clearly, we have to prevent that if we can, and the best way is to keep that person from having a security clearance.

Unexplained affluence is also a major concern.

The second type of information deals with what's called "unexplained affluence." Simply put, unexplained affluence means living better than you should, given your known means. For example, a GS-5 who owns a yacht is a case of unexplained affluence. The credit report can reveal unexplained affluence by reporting that subject has monthly credit card payments of \$2,000.00, and is meeting them. You know that the subject is single and makes \$18,000.00 a year. Clearly, there's an issue here that needs to be resolved. Probably, the subject has an inheritance or won the lottery or something. Possibly, though, he/she has become involved in espionage or drug dealing, or some other situation which makes his/her loyalty, reliability and trustworthiness questionable.

Most of the information in most credit reports will be of no adjudicative interest at all. Remember, though, we're looking for that 5% or so of people who shouldn't and won't get clearances, and the credit report will help us find them.

The credit report is one of the most important tools available to you as an adjudicator. The typical American who becomes involved in espionage does it for the money. It can help identify people whose financial situation is such that they might be motivated to sell out their country.

You can expect to see credit reports in the SSBI, PR, ANACI and NACLCL. Occasionally, they're also in SIIs. Currently, the NAC doesn't contain a credit report.

DSS and OPM obtain credit reports through a credit vendor, who provides national credit coverage through the major credit bureaus. This ensures that the best available information is provided to you.

DSS will provide the actual credit report in all PSI containing a credit check. Otherwise, the credit report is destroyed and you are notified of a favorable result.

OPM will always provide a copy of the credit report, even if it's favorable.

The credit report is a prime source of information on both bad debts and unexplained affluence, two of the most important considerations in security eligibility.

Review Exercise

1. Which agencies are authorized to conduct PSIs for the DoD PSP?

2. DSS jurisdiction is limited to DoD affiliated personnel in the 50 states, the District of Columbia, and Puerto Rico.

- a. True
- b. False

3. Questions asked in the course of a PSI must be reasonably expected to develop information which is _____ and _____ to making a personnel security determination.

4. List five of the nine investigative techniques DSS must avoid using.

- 1. _____
- 2. _____
- 3. _____
- 4. _____
- 5. _____

5. Beside each situation shown below, write the necessary PSI:

- a. Secret clearance for a contractor: _____
- b. Civilian employee in a critical-sensitive position: _____
- c. Military member with Secret clearance requirement: _____
- d. To resolve issues raised about a subject's security eligibility: _____

6. The Subject Interview is routinely a part of which two PSIs?

- 1. _____
- 2. _____

7. Identify the PSIs whose scope and period of coverage are shown below:

- a. Last Five Years
NAC
Employment Records
Supervisors
Education Records
Listed Character References
LACs
Credit Checks

Answer: _____

- b. Last Five Years
NAC
Spouse NAC (if we don't have on file)
Subject interview
Employment Records

Employment Interviews
Developed Character References
Neighborhood Inquiries
LACs
Credit Checks

Answer: _____

8. What are the three most common errors found in PSI requests?

1. _____
2. _____
3. _____

9. What is the major problem with the NAC?

10. What two types of information will a credit report usually reveal?

1. _____
2. _____

11. What are three of the five major problems with the ANACI & NACI?

- 1. _____
- 2. _____
- 3. _____

12. OPM will resolve only employment suitability issues raised in an ANACI or NACI.

- a. True
- b. False

13. List the three agencies always checked in a NAC.

- 1. _____
- 2. _____
- 3. _____

14. Which agency was established as DoD's single centrally directed personnel security investigative service by the 5200.2-R?

15. OPM will expand the ANACI to resolve any security related issues.

- a. True
- b. False

16. Which PSIs are conducted on civilians only?

17. Which PSIs routinely contain credit reports?

18. What are the three national credit bureaus checked by the DSS credit vendor?

1.

2.

3.

19. A Personnel Security Investigation is an inquiry into someone's:

20. What are the three investigations authorized for the initial issuance of a security clearance eligibility?

Solutions & References

1. DSS and OPM (Lesson 3, page 3-3)
2. a. True (Lesson 3, page 3-7)
3. relevant and necessary (Lesson 3, page 3-14)
4. (Lesson 3, page 3-11)
 1. Using mail covers(reviewing incoming & outgoing mail)
 2. Conducting physical surveillance
 3. Conducting photographic surveillance
 4. Conducting physical searches
 5. Using voice analyzers
 6. Inspecting trash
 7. Using paid informants
 8. Using wiretaps
 9. Using eavesdropping devices
5. (Lesson 3, page 3-19)
 - a. NACLC
 - b. SSBI
 - c. NACLC
 - d. SII
6. (Lesson 3, page 3-36)
 1. SSBI
 2. PR

7.
 - a. ANACI (Lesson 3, page 3-30)
 - b. NACI (Lesson 3, page 3-30)
 - c. PR (Lesson 3, page 3-32)

8. (Lesson 3, page 3-45)
 1. Incomplete Information
 2. Discrepant Information
 3. Deliberate Falsification

9. The Scope. A NAC is not designed to develop information, but rather to consolidate existing information. It only taps existing federal record banks and consolidates the information found into a single report. (Lesson 3, page 3-48)

10. (Lesson 3, page 3-62)
 1. Bad Debts
 2. Unexplained Affluence

11. (Lesson 3, page 3-49)
 1. Primarily an employment investigation (NACI only)
 2. No field investigation conducted
 3. No context for sources' comments
 4. Failure to resolve issues
 5. The Subject "controls" the investigation.

12. a. True (Lesson 3, page 3-49)

13. (Lesson 3, page 3-28)
 1. DCII
 2. FBI/HQ
 3. FBI/ID

14. The Defense Security Service (DSS) (Lesson 3, page 3-7)

15. False (Lesson 3, page 49)

16. NACI & ANACI (Lesson 3, page 3-21)

17. SSBI, ANACI, NACI, NACLC (Lesson 3, page 3-56)
18. TRANS UNION, Experion, Equifax (Lesson 3, page 3-57)
19. Background, Lifestyle, Personal History (Lesson 3, page 3-14)
20. SSBI, ANACI, NACI (Lesson 3, page 3-16)

LESSON 4

CENTRALIZED ADJUDICATION

In the previous lessons, we looked at two of the four elements of the PSP. In Lesson 2, we discussed how positions are designated. The PSIs required for each type of position were addressed in Lesson 3. In this lesson, we will begin to look at the third element of the PSP-- **Adjudication**. Figure 4-1 identifies the "whole person" concept in making personnel security determinations.

Adjudication

- **Evaluation of “whole person”**
 - ◆ **Favorable information**
 - ◆ **Unfavorable information**
 - ◆ **Circumstances**
- **Use adjudication guidelines**
- **Adjudication is to determine**
 - ◆ **Loyalty**
 - ◆ **Trustworthiness**
 - ◆ **Reliability**



3

Figure 4-1

We will view it from the perspective of the functions that a Central Adjudication Facility (CAF) performs and your responsibilities as an adjudicator. The confidentiality of personal information contained in PSIs will be discussed. The CAF's role in Special Access Programs and procedures for carrying out adverse personnel security determinations will also be addressed.

Why do we have CAFs? Prior to centralizing the adjudicative function within each Component, each activity commander was responsible for making adjudications on assigned personnel. This led to duplication of effort since many commanders decided to re-adjudicate a PSI on new personnel even if the previous commander had adjudicated the same PSI. There was no training available for activity personnel to help them make adjudicative determinations. This often resulted in different decisions based on the same PSI--there was no consistency of adjudicative determinations.

Finally, there were no centrally available records that could provide accurate information on the overall personnel security program. In 1975, DoD decided to have the Components centralize the adjudicative function into one facility within each Component. Each Component has now centralized. Centralization is designed to provide consistency in adjudicative determinations and eliminate the duplicative efforts by activity commanders. A central data base of personnel security information provides management data for the Components, DoD and other authorized requesters.

We will look at **your** role in the CAF. Your responsibilities and limitations direct what you can do and how you do it. What is the effect of bias on your determination and what is the impact of your determination on the subject?

A responsibility of persons who have access to PSIs is to protect the sensitive personal information contained in the investigations. The Privacy Act establishes requirements for the collection, use and dissemination of personal information. The Privacy Act protects personal information in PSIs. The information may only be used for official purposes and may be released to persons with a need-to-know. The investigative agency is the only one authorized to release a PSI directly to the subject. Each CAF has internal procedures for handling PSIs and who may have access to them.

A Special Access Program is established to control access, distribution and protection of particularly sensitive information. CAFs make the personnel security determinations for security clearance or sensitive duties

for these programs. Certain CAFs make eligibility determinations for access to SCI. A program manager outside of the CAF will make the final determination of acceptance or retention in the program.

A major responsibility of a CAF is taking action to deny or revoke a security clearance or eligibility to perform sensitive duties. The procedures used to carry out this action make up the "due process" a subject receives. The procedures call for a notice to the subject of the proposed action, an opportunity to reply, a final decision and the opportunity to appeal an unfavorable decision.

Each of these areas will be discussed in this lesson.

THE ADJUDICATOR'S RESPONSIBILITIES

In this section, we will look at your responsibilities as an adjudicator. We will look at the different conditions that influence how you carry out your responsibilities. Your grade level may determine what types of cases and actions you can approve and which ones must be referred to a more senior adjudicator.

Once your duties have been assigned, what are the considerations involved in adjudications? We will look at the relevancy of information and the thirteen adjudication guidelines to help you evaluate the information. Each adjudication guideline is divided into disqualifying and mitigating conditions to help you evaluate that type of information.

We will also look at personal bias and how it could affect your adjudication. Once your decision has been made, you will see the impact that a favorable or unfavorable determination can have on the activity and the subject.

Finally, we will look at the functions a Central Adjudication Facility (CAF) provides and your role in the CAF.

Finally, we will look at the functions a Central Adjudication Facility (CAF) provides and your role in the CAF.

READING ASSIGNMENTS

DoD 5200.2-R Chapter 2: Paragraph 2-504

DoD 5200.2-R Chapter 3: Section 5

DoD 5200.2-R Chapter 5: All

DoD 5200.2-R Chapter 6: All

DoD 5200.2-R Chapter 7: All

DoD 5200.2-R Chapter 9: Section 1

DoD 5200.2-R Appendix F: All

Memo: Pers Scty Inves and Adj

THE PERSONNEL SECURITY ADJUDICATOR

The personnel security adjudicator plays an important role in the DoD Personnel Security Program. As an adjudicator, you are primarily responsible for initial and subsequent personnel security determinations on DoD affiliated personnel who will require access to classified information or perform sensitive duties.

The decisions you make have short and long-term effects on both the national security and the subject. DoD has established criteria and adjudicative guidelines to assist you in reaching a final decision.

In making a determination, you must apply the criteria, guidelines, knowledge of the program, experience and common sense. Before arriving at a decision, all of the facts and circumstances contained in each PSI must be weighed on its own merits

Adjudicative Factors

- **Nature, extent, and seriousness of the conduct**
- **Circumstances**
- **Frequency and recency**
- **Age and maturity**
- **Voluntariness of participation**
- **Rehabilitation**



4

Figure 4-2

Adjudicative Factors

- **Motivation for the conduct**
- **Potential for**
 - ◆ **Pressure**
 - ◆ **Coercion**
 - ◆ **Exploitation**
 - ◆ **Duress**
- **Likelihood of continuance or recurrence**



5

Figure 4-3

In addition to the adjudicative factors, the adjudicator, must review actual or potentially derogatory information

about the individual and consider the information in Figure 4-4.

Additional Considerations

Questions to be asked about the individual:

- **Voluntarily reported information**
- **Truthful & complete in responding to questions**
- **Sought assistance & followed professional guidance**
- **Resolved or appears likely to resolve the security concern**
- **Demonstrated positive changes**
- **Should access be temporarily suspended**



6

Figure 4-4

In recent years, the emphasis has been on centralizing the adjudicative function in each DoD Component. The Components are now required to centralize this function and have either completed centralization or are in the process of centralizing.

RESPONSIBILITIES OF THE ADJUDICATOR

Your role in the personnel security program is that of making personnel security determinations which allows access to classified information or assignment to sensitive duties. The decision made by you is accepted throughout the DoD as the basis for certifying eligibility for security clearance or sensitive duties. This decision permits the subject's commander to grant access to classified information or perform sensitive duties. The decision also permits commanders of other DoD activities to grant access to

classified information to the subject or permit him/her to perform sensitive duties when temporarily assigned to another command.

In this role, you must review PSIs and other information based on a common-sense evaluation by applying the adjudicative criteria and guidelines.

The following is a listing of some of the adjudicator's responsibilities.

- * Authorizing security clearances or eligibility determinations to perform sensitive duties;
- * Adjudicating PSIs;
- * Adjudicating supplemental information;
- * Requesting additional information/investigation to resolve issues;
- * Initiating loyalty reviews;
- * Initiating actions to deny/revoke a security clearance or eligibility to perform sensitive duties;
- * Taking final actions on decisions to deny/revoke a security clearance or eligibility to perform sensitive duties;
- * Ordering temporary suspension of access to classified information pending final resolution of issues;
- * Maintaining personnel security records/files;
- * Making reports of personnel security information;
- * Providing interrogatories/depositions or testifying before hearings, boards, courts or other administrative bodies to explain personnel security determinations;
- * Providing information on personnel security policies and procedures to requesters;

- * Notifying investigative agencies of certain types of information; and
- * Referring certain suitability issues to personnel authorities for military retention or civilian employment determinations.

ADJUDICATION OF PSI's

During the actual adjudication of a PSI or other information, several conditions must be considered:

- * Is the PSI complete and ready for adjudication?
- * Are there any basic qualification issues in the PSI that would cause referral to personnel authorities for military retention or civilian employment decisions?
- * Is the information complete so that all potential issues are resolved?
- * When considering the information in the PSI, is it relevant?
- * The actual decision process consists of weighing the information, both favorable and unfavorable, against the adjudicative criteria and guidelines.
- * The final decision must be that a favorable determination is in the interests of national security.
- * Personal bias must not influence the adjudication.
- * Classified and personal information must be protected.

THE COMMON-SENSE APPROACH

When making a determination, you may only consider information that is relevant to a personnel security determination. Other matters that would not directly impact on the personnel security determination are not appropriate for consideration in the adjudicative process.

For example, the subject's religious beliefs are not normally a proper area of consideration. A belief in some form of supreme being is not an adjudicative issue by itself because it does not reflect on the subject's loyalty, trustworthiness or reliability. If the religious practices involve the violation of public laws, such as harboring and protecting illegal aliens, then the relevancy of the information for adjudication has been established because the subject's trustworthiness is now questioned due to criminal conduct.

Adjudication guidelines are aids providing policy guidance to help you evaluate different types of information in determining eligibility for clearance or sensitive duties. **The adjudicative guidelines contain disqualifying and mitigating conditions which are critical to the adjudicative process.**

The concept is that a disqualifying condition is one that the conduct is so serious that it could be the basis for an adverse personnel security determination. A mitigating condition lessens the severity or seriousness of a disqualifying condition to the point that a favorable determination may be possible. Figure 4-5 shows the adjudication guideline structure.

Adjudication Guideline Structure

- **Basis - what the guideline covers**
- **Disqualifying Conditions**
 - ◆ **Serious enough to be disqualifying**
 - ◆ **One or more conditions may apply**
- **Mitigating Conditions**
 - ◆ **Reduces the seriousness**
 - ◆ **May or may not be present**
 - ◆ **May or may not outweigh the disqualifying information**

8

Figure 4-5

The disqualifying and mitigating conditions are not absolutes. They cover most of the information you will see, but occasionally the circumstances will not fit into the guidelines.

If you are not sure, ask a senior adjudicator or your supervisor about it.

A multiple issue PSI is more complex because disqualifying conditions from different guidelines are present in the case and there may be mitigating conditions present from different guidelines. The conditions of each case and their interrelationships will affect the final decision based on that particular set of facts and circumstances.

Your final decision is whether it appears the subject can reasonably be expected to properly safeguard classified information or perform sensitive duties. If there is a question about the subject, a favorable determination cannot be made. The adjudication guidelines and disqualifying and mitigating conditions will be discussed in detail in Lesson 5.

Your experience, knowledge of similar cases, and general application of the guidelines is a process of applying logic to the decision-making process.

A single adjudication guideline to cover all aspects of human behavior is not possible; therefore, reliance is placed on you to think the information through and arrive at the decision through the exercise of sound judgment and careful analysis.

Because we are dealing with people, common sense is an integral part of adjudication. People change and those changes may affect their initial or continued eligibility to hold a security clearance or perform sensitive duties.

You must keep this in mind when making determinations. **You are being asked to make a determination about the future based on the past and, in some cases, the individual's stated intent about future actions.** These statements may be a sincere statement of intent or an attempt to deceive. This is where duties of the position and adversely impact on his or her short and long-term career. It could delay advancement and it could even cause a change in career fields if the subject cannot work. Careful analysis of the information, along with experience and common sense, will help you to make the final decision.

IMPACT OF ADJUDICATION

The adjudication is designed to protect the interests of national security, but you must also consider the impact on the subject. A favorable decision will permit the subject to continue a civilian or military career of employment on classified contracts. An unfavorable decision can have several different effects on the subject.

At the minimum, it will cause the subject to be ineligible to perform the duties of the position and adversely impact his/her short or long-term career. It could delay advancement and it could even cause a change in career fields if the subject cannot work without a favorable personnel security determination.

For military personnel, this could cause a change in the Military Occupational Specialty (MOS) or rating. Civilian personnel would not be eligible to occupy a sensitive position, but could occupy a nonsensitive position. Contractor personnel would not be eligible for access to classified information within DoD.

At the maximum, an adverse determination can indirectly cause the loss of civilian employment, release from military service, or termination of work on a particular contract.

An adverse loyalty decision could be the direct cause of loss of civilian employment or discharge from military service. **In certain cases, the information that caused the unfavorable determination could even be the basis for criminal prosecution under United States law or the Uniform Code of Military Justice.**

THE ROLE OF BIAS IN ADJUDICATIONS

One of your most important responsibilities as an adjudicator is to ensure that **“each adjudication is...an overall common-sense determination based upon consideration and assessment of all available information.”** This requires that all of your decisions be reasoned, rational and thought out. Because of this, **adjudicators can't let their personal feelings, biases, and prejudices** enter into the decision making process. Personal bias is simply not acceptable in adjudicative determinations.

There are a number of ways that personal feelings can enter the adjudicative process: you may have a prejudice (preconceived opinion or judgment) against members of a particular racial or religious group; you may have a bias (an inclination of temperament or outlook) in favor of people with a particular educational or employment history; or you may have personal feelings based on an experience you have shared with the subject.

Any of these can be either positive or negative. **Just as you can be prejudiced or biased against someone, so you can be prejudiced or biased in favor of someone.** You may identify favorably with the subject because you and he/she have shared some experience, such as divorce, so you can also identify with the victim of subject's actions - for instance, if subject is a child abuser, and you were an abused child.

Regardless of whether your bias is positive or negative, it is unacceptable. Figure 4-6 contains a listing of some biases which can influence your adjudications. When your determinations are influenced by personal bias, you are unable to make sure that "each adjudication...is based upon consideration and assessment of all available information." Rather, your adjudication is being driven by only one piece of information - by the subject's race or by the fact that subject is a child abuser.

When you allow bias to influence your decision, you are adjudicating subject as a member of a group or class rather than as an individual. This is the quickest way for both you and your CAF to end up in very hot water.

COMMON BIASES WHICH CAN AFFECT ADJUDICATIONS

- * **Prejudice based on racial, ethnic or religious background**
- * **Prejudice against homosexuals**
- * **Prejudice based on subject's history as a child molester or abuser**
- * **Prejudice against someone because of prior criminal activity, such as rape or drug dealing**
- * **Prejudice for or against subject because of substance abuse**
- * **Identifying with subject because you and he/she have shared experiences or background**
- * **Identifying with the victims of subject's actions**

Figure 4-6

As an adjudicator you have a responsibility to identify your own biases, prejudices, and understand when your personal feelings are likely to affect your professional judgment. And having done that, you have to put a tight rein on these biases and feelings. This doesn't mean that you have to squelch all human feelings in order to be a good adjudicator. It does mean that you have to keep them in perspective and recognize them for what they are: **personal** feelings and opinions which can't be allowed to influence **professional** judgments and decisions.

CENTRAL ADJUDICATION FACILITIES (CAFs)

Final adjudications are done at the CAF.

CAFs have been established to perform the personnel security adjudication function for each component. Some of the major functions a CAF performs for its Component are:

- Authorize security clearances and eligibility determinations to perform sensitive duties;
- Deny or revoke security clearances or sensitive duty eligibility determinations;
- Maintain a central data base of personnel security investigative and adjudicative information;
- Provide management data upon request;
- Provide information to local commands on procedures for requesting PSIs and adjudications;
- Review and adjudicate supplementary information as part of continuous evaluation;
- Review and adjudicate Periodic Reinvestigations (PR). Some CAFs provide local commands information on when PRs are due on subjects;
- Provide adjudicative information to the Defense Clearance and Investigations Index (DCII) for use by all DoD components;
- Implement procedures for protecting classified and personal information held by the CAF; and
- Other functions as assigned by the Component.

PERSONNEL SECURITY DETERMINATIONS FOR SAPs

CAFs make the personnel security determinations for individuals nominated for SAPs. Within DoD, CAFs also make the access determination for the SCI program per the criteria of Director of Central Intelligence Directive 6/4 (DCID 6/4). This is accomplished by either one CAF making both determinations or by separate CAFs. One CAF making the determination for the security clearance and the other for the SCI access determination.

The following is a list of CAFs who make SCI access determinations:

- Army Central Clearance Facility
- Navy Central Adjudication Facility
- Air Force Central Adjudication Facility
- Defense Intelligence Agency
- National Security Agency

THINGS TO REMEMBER

You have many responsibilities assigned and functions to perform in fulfilling your role in making final determinations which permit commanders to grant access to classified information or assign personnel to sensitive duties. The type of actions you may take will depend upon the type of PSI, action needed, and the organization of the CAF.

When working in a CAF, you may perform any or all of these functions. This will be decided by the administrative organization of the CAF and your grade level. Once your duties have been determined, you will be delegated the authority to perform those responsibilities and functions.

There are certain limitations placed on you to ensure that the information considered is relevant and that information contained in the PSI is properly protected.

There are several considerations involved in making an adjudicative decision: the appropriateness of the request; a complete PSI; equal consideration of all information; the decision is free from personal bias; the information considered is relevant to the decision; the final decision must support the interests of national security. Also, the impact on the subject must be considered as the determination can have positive and negative effects on the subject's current and future career.

The adjudicative process is centralized in each DoD Component. The CAFs provide personnel security services for the Component. The adjudicator in a CAF may perform a variety of functions depending upon the organization and type of PSIs/actions involved.

CONFIDENTIALITY OF FILES

As an adjudicator, you will review PSI's that contain personal information regarding subjects. The information is provided for use in determining a subject's eligibility for a security clearance and assignment to sensitive duties. You must ensure this information is tightly controlled and not made available to any person or organization which does not have an official need-to-know it. We will examine the protection of personal information and the subject's access to it.

PROTECTION OF PSIs AND OTHER INVESTIGATIVE REPORTS

Information contained in PSIs and other investigative reports requires protection based on the category of the information. The information is generally in two categories.

The first category of information is unclassified but personal in nature and is protected by the provisions of the Privacy Act. This law establishes requirements for protecting personal information collected, held and used by the United States government. You must protect personal information on individuals. DoD Directive 5400.11, Department of about the subject. Defense Privacy Program, implements the Privacy Act in DoD.

The second category is classified information which is protected by the requirements of DoD 5200.1R, Information Security Program Regulation. This directive establishes procedures for the handling, storing and dissemination of classified information.

We will address the basic procedures for safeguarding information you will see when reviewing PSIs and other information.

PROTECTING CLASSIFIED INFORMATION IN PSIs

Occasionally, you will see a classified PSI. PSIs containing classified information must be protected in accordance with the requirements of DoD 5200.1R and the Component regulations that implement it.

PSIs containing classified information are treated the same as any other classified document for purposes of storage, retention, safeguarding and dissemination. This depends on the classification level. When handling classified PSIs, you must ensure that the report is released only to persons within the CAF with an official need-to-know and the proper security clearance.

Each CAF has internal procedures established to control the classified PSIs while they are at the facility. If a classified PSI is sent to a local command or other DoD component, that command or component is responsible for its proper protection.

COLLECTION OF PERSONAL INFORMATION

PSIs and other information about subjects which is considered by you as personal in nature are protected by the Privacy Act, DoD Directive 5400.11, and the Component regulations.

The collection of personal information by the United States government is controlled by the Privacy Act. The Act sets forth a requirement to publish in the Federal Register all systems of records for which personal information is collected. This permits the general public to be aware of official systems of records that maintain personal information and the specific uses of the information.

Each time a Federal agency wishes to collect personal information, a written Privacy Act notification must be provided to the subject notifying him/her why the information is being collected, its routine uses, and the impact of failure to provide the requested information. Lesson 2 identified the various forms used to collect personnel security information.

What is **personal** information that is covered by the Privacy Act? Personal information is that information which is intimate or private to the subject. Information that is related solely to the subject's official functions or public life is not covered by the Privacy Act.

Some examples of personal information are:

- **Social Security Number**
- **Date and place of birth**
- **Home address**
- **Home telephone number**
- **Financial information**
- **Medical information**
- **Counseling records**

Personal information is collected from military and civilian personnel to conduct PSIs for military retention and civilian employment determinations.

For personnel security purposes, we collect personal information from subjects to use in making a personnel security determination. The same investigation used for a retention or employment determination is, in many cases, also used for the personnel security determination.

ACCESS TO INVESTIGATIVE FILES AND INFORMATION

Personal information contained in PSIs and other investigative files may be released to those government officials who must see the information to perform their duties.

These are usually officials who must make civilian employment/military retention decisions (including the current supervisor), personnel security determinations or perform other functions indirectly affecting employment, retention or security determinations.

Remember, you are the custodian, not the owner of the report. Figure 4-7 shows some of these individuals who may need official access to the Personnel Security Investigations information.

Personnel with Official Need To Know

- **Supervisors**
- **Medical personnel**
- **Military & civilian personnel officials**
- **Security/law enforcement/CI officials**
- **Special programs (SCI, PRP, etc.)**
- **Hearings and Boards**



Figure 4-7

In all of the above cases, the individual(s) must have an **"OFFICIAL NEED TO KNOW"** - not just idle curiosity. An example would be a medical determination for continued employment/military retention or security clearance/assignment to sensitive duties. For example, a physician would be requested to review the personal information in the PSI, and provide medical information necessary for the military personnel officer to make a retention decision.

The PSI contains information that the subject is a paranoid schizophrenic with probability of recurring violent episodes. The physician's opinion is that the subject is not suitable for retention because of the medical condition. The subject is then discharged. The information in the PSI was provided to an authorized official for a medical opinion.

The use of the PSI by other officials also occurs when a program has additional requirements beyond the personnel or security determinations. An example of this would be the nuclear Personnel Reliability Program (PRP). The commander is responsible for making the PRP certification. He must review the PSI or other investigative files in order to make a decision on the certification independent of the personnel security determination by the CAF.

TRANSMITTING PSIs

A PSI or other investigation conducted by a DoD investigative agency may be transmitted within DoD for official use, generally without prior approval of the investigative agency. In some cases, the investigative agency may place restrictions on dissemination beyond the original requester due to current criminal, counterintelligence or prosecutorial considerations. If this is the case, the investigative file will contain specific instructions on its handling and dissemination.

An investigative file created by a DoD investigative agency may not be provided to another Federal agency without the approval of the agency that did the investigation.

For example, if the Department of Energy (DOE) requests a DSS file on a new employee who previously worked for a DoD Component, the holder of the file could not send the file directly to DOE. DSS would have to approve of the release to a non-DoD agency and provide a copy of the file to DOE.

PSIs conducted by OPM are handled in the same manner as DSS PSIs. All of DoD is considered one agency for file handling purposes by OPM. An OPM PSI may be transmitted within DoD without further approval of OPM. If another Federal agency needs an OPM PSI, the DoD component can not release the file directly to the agency. The agency would request a copy of the file from OPM and they would make the release.

RELEASE OF PSIs TO THE SUBJECT

A DSS or OPM PSI, or other investigative file, may be released only to the subject of the investigation or his/her designated representative by the investigative agency. See Figure 4-8.

Release of Report

- You are the *custodian*, not the owner
- May be released only by the investigating agency
- Subject or representative may not be given direct access
- Individuals who have no need to know should never be given report
- Privacy Act & Freedom of Information Act procedures apply.



5

Figure 4-8

This is necessary to protect information in the file that may not be releasable to the subject, such as classified information or confidential sources. Only the investigative agency is in a position to make this determination.

The current holder of an investigative file *cannot* provide the file, or any part of it, directly to the subject.

If a subject requests a copy of the file, he/she should be advised to write to the investigative agency requesting a copy. The investigative agency will treat the request under the procedures of the Privacy Act for release.

HEARINGS and BOARDS

There are situations where an adverse action may be proposed against a subject and the procedures of that action permit the subject to be given a copy of all information being used in the proposed action.

If the action, such as a removal from civilian employment or discharge from military service involves information in a PSI or other investigative file, the subject may not be given the file, directly or indirectly, without the investigating agency's approval. This may be accomplished by notifying the investigative agency prior to the board or hearing date. Explain that information in the PSI will be used in a board or hearing and a release authorization is necessary before the information can be presented or released to the subject. The investigative agency will provide the file, or portions of it. The subject must not be given a copy of the file (including the copy used by the hearing or board) unless the approval has been received from the investigative agency.

RELEASE OF INFORMATION AND PENALTIES

Penalties

- **Giving someone access without official need is violation of Privacy Act**
- **Maximum \$5,000 fine**
- **Disciplinary action by agency**



Figure 4-9

Any release of information for purposes other than that for which it was collected requires a written notification to the subject of why it was released and to whom. **The Privacy Act provides penalties for unauthorized release or disclosure of protected information.** If the protected information is improperly released to unauthorized individuals, the person who released it may be fined up to \$5,000 per offense by a Federal court.

A person improperly releasing protected information is also subject to adverse administrative actions by his/her Component.

If you receive a request for a release of personal information, give it to your supervisor. He/she will see that it is handled per your Component procedures.

DUE PROCESS

Now, you will learn the procedures to deny or revoke a security clearance, Limited Access Authorization (LAA) or eligibility to be assigned to sensitive duties. The procedures are called "**due process.**" They are intended to inform the subject of a proposed unfavorable administrative action and permit him/her to reply with reasons why the action should not be taken. The procedures also offer an appeal if the CAF determination is unfavorable.

This is how to say "No"

The CAF has decided to make an unfavorable personnel security determination. To implement this determination, the CAF must take an unfavorable administrative action.

The procedures to carry out this action are called "**due process.**" These procedures must be followed to deny or revoke a security clearance (military, civilian and contractor) or determine the subject ineligible to be assigned to sensitive duties (military and civilian).

The following paragraphs outline the basic procedures for administering due process. You will notice a difference in due process between military/civilian and contractor personnel. The military/civilian program is governed by

administrative policy of DSP, ODASD(CI&SCM) while the contractor program conforms to the specific requirements of E.O. 10865.

Figure 4-10 shows how the procedures for due process are determined by the program and the person's status.

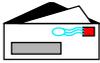
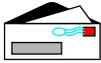
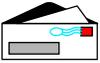
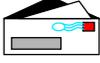
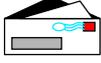
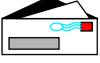
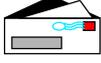
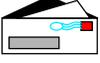
Due Process				
Status	DoD 5200.2-R	DCID 6/4	DoD 5220.6	DoD-O 5205.7
			N/A	
			N/A	
	N/A			

Figure 4-10

DoD 5200.2-R governs security clearance and sensitive duties procedures for military and civilian personnel.

DoD 5220.6 governs security clearance procedures for contractor personnel.

Director of Central Intelligence Directive 6/4 (DCID 6/4) governs SCI procedures for all personnel.

DoD Directive O-5205.7 governs SAP procedures for all personnel.

DUE PROCESS FOR MILITARY AND CIVILIAN PERSONNEL

Due process must be given to military and civilian personnel to deny or revoke a security clearance, deny or revoke an LAA, or declare the subject ineligible to perform sensitive duties. These procedures are administrative in nature and are in writing.

A personal appearance before a Administrative Judge can be offered in these proceedings. The procedures are shown in Figure 4-11.

Due Process-Military/Civilian

- CAF sends Statement of Reasons (SOR)
- Person may reply
- Command position
- CAF considers reply and command position
- Final decision
- Appeal
 - ◆ Decision by PSAB , or
 - ◆ Personal appearance with recommendation to PSAB



Figure 4-11

The Central Adjudication Facility (CAF) sends a **Statement of Reasons (SOR)** indicating the reasons for the proposed action.

The **person may reply** to the SOR but is not required to reply.

The **command may place its position** with the person's reply to the SOR.

The **CAF considers the reply and the command's position.**

If the decision is negative, a Letter of Denial/Revocation (LOD) is sent via the command to the person indicating the final CAF determination.

The **person may choose to appeal** to the Personnel Security Appeal Board (PSAB) with:

- A decision by the PSAB based on review of the appeal, or
- **Request a personal appearance.** The personal appearance (explained in Figure 4-12 below) gives the person the opportunity to explain or provide information to an Administrative Judge (AJ) from the Defense Office of Hearings and Appeals (DOHA).
- The AJ then makes a recommendation to the PSAB.
- The PSAB considers the appeal and the AJ recommendation.
- The person is notified of the final determination.

Personal Appearance

- Option when denied/revoked by CAF.
- An Administrative Judge from DOHA
- Receives information from person in written or verbal form.
- Makes written recommendation to PSAB within 30 days after appearance.



Figure 4-12

If the decision is favorable, the CAF decision is overruled and the subject declared eligible to hold a security clearance or be assigned to sensitive duties.

If the decision is unfavorable, the CAF decision is upheld. The appeal decision is the last action on the personnel security determination within the Component. The subject, the activity and the CAF are notified in writing of the appeal decision.

CONTRACTORS

Due process is given to a contractor employee to deny or revoke a security clearance. The Defense Office of Hearings and Appeals (DOHA), is the CAF that administers due process to all DoD contractors for security clearance denials or revocations. The procedures are:

- * DOHA issues a Statement of Reasons (SOR) to the contractor employee. The SOR provides the reasons for the proposed action as specifically as national security and privacy considerations permit.
- * The subject may choose to reply to the SOR. If the decision is favorable, the contractor employee is declared eligible to hold a security clearance. If not, the subject may request a hearing before an Administrative Judge (JA)

(Note: The "Adjudication Policy" contained in Enclosure 3 of DoD 5220.6, has been superseded. The adjudication policy guidelines of DoD 5200.2-R are now used to evaluate information.)

- * If requested, a hearing will be scheduled. The AJ will conduct the hearing and permit the subject and government to call witnesses and present evidence or other information. Department Counsel will represent the government in these hearings.
- * If the AJ's decision is favorable, the subject is eligible to hold a security clearance. If not, the subject may appeal to the Appeal Board.
- * Department Counsel may appeal a decision in favor of the subject to the Appeal Board.
- ◆ The Appeal Board will review the case and make a determination. This determination is the final action on the security clearance. Figure 4-13 outlines the due process procedures.

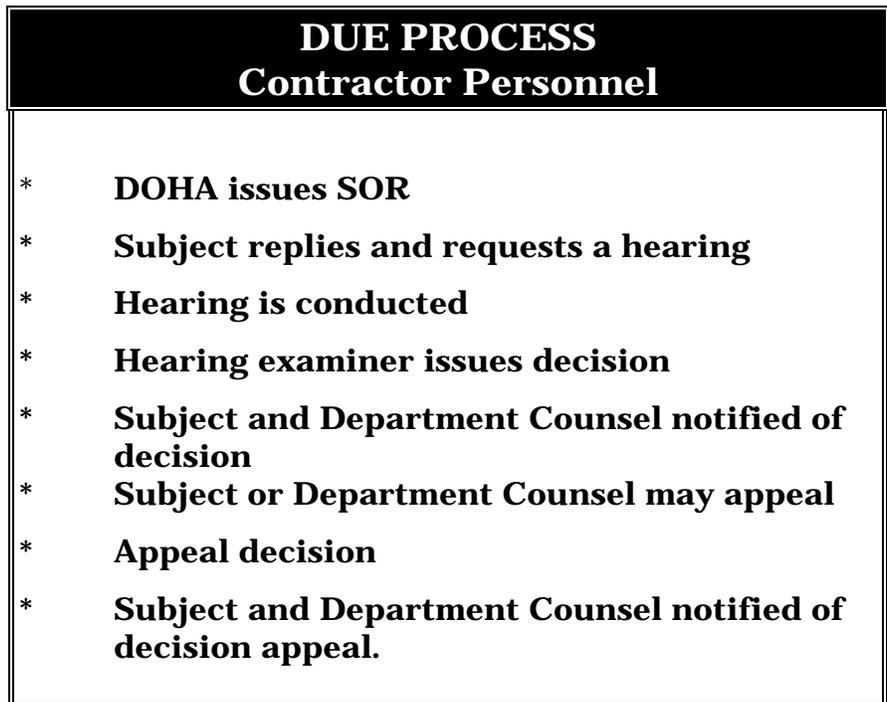


Figure 4-13

RECONSIDERATION

Taking another look at an unfavorable decision.

Each Component has procedures for reconsideration of an adverse personnel security determination. **These procedures allow for a review of an unfavorable determination, usually after at least one year**, if the activity believes the reasons for the initial adverse decision have been overcome and the subject would now be eligible.

A subject is not entitled to due process on reconsideration as he/she has already received it with the original determination. Consult your Component regulation for specific procedures.

APPLICABILITY

Due process must be given to U.S. citizens and immigrant aliens nominated for, or currently holding, a security clearance, LAA or assignment to sensitive duties.

Foreign nationals are not entitled to due process for an LAA.



SUMMARY

You will have many responsibilities working in a CAF. The adjudicative actions will vary depending upon the type of Personnel Security Investigations, the actions required to make a final determination and, of course, the structure of your CAF.

Equal consideration must be given to all information in the case without bias based on the whole person concept. Your final decision must support the interests of national security.

This lesson identified the procedures required for a CAF to take a final unfavorable administrative action leading to the denial or revocation of security clearance, LAA or eligibility to be assigned to sensitive duties for military and civilian personnel.

For contractors, the procedures for denial or revocation of security clearance are administered by DOHA. The requirement for due process applies to U.S. citizens and immigrant aliens.

These procedures ensure that the subject is informed of the reasons for the proposed action and is given the opportunity to reply with information he/she wishes the CAF, Appeals Board or Administrative Judge to consider in making a final decision. Also, it offers the opportunity to appeal an unfavorable decision by the CAF or Appeals Board.

Review Exercises

- 1. Requests for PSIs may be submitted for any reason by the subject's supervisor.**
 - a. True
 - b. False

- 2. Which of the following is a function of a CAF?**
 - a. Making final appointments to civilian sensitive positions after completion of the PSIs.
 - b. Denying or revoking security clearance and sensitive duty eligibility.
 - c. Making final determinations on appeals of denied or revoked security clearances
 - d. Determining a subject's eligibility for military service.

- 3. The security clearance of a military member may be revoked by the Defense agency he/she is currently assigned to.**
 - a. True
 - b. False

- 4. On which PSI request package is a supervisor required to place a statement of whether he/she knows of derogatory information?**
 - a. NAC
 - b. SSBI
 - c. PR
 - c. SII

- 5 Each adjudication guideline is divided into which two sections?**
- a. Loyalty and suitability issues
 - b. Disqualifying and mitigating conditions
 - c. Trustworthiness and reliability standards
 - d. Judgment and reliability standards
- 6. Which of the following is NOT a responsibility of an adjudicator?**
- a. Authorizing security clearances or eligibility determinations to perform sensitive duties.
 - b. Requesting additional information/investigation to resolve issues.
 - c. Initiating actions to deny or revoke a security clearance or eligibility to perform sensitive duties.
 - d. Authorizing retention in military service or civilian employment.
- 7. A mitigating condition does which of the following?**
- a. Overcomes a disqualifying condition in every case and permits a favorable determination.
 - b. Lessens the severity or seriousness of a disqualifying condition.
 - c. Has almost no effect on the final determination.
 - d. The adjudicator may consider it to decide a "borderline" case.
- 8. _____ is the means by which personal feelings, prejudices and beliefs can influence an adjudication.**

9. To the greatest extent practical, personal information relevant for a security determination should be obtained from which of the following?

- a. Employers
- b. Law enforcement agencies
- c. Subject
- d. Credit bureaus

10. If the subject refuses to provide a Standard Form 86 needed for requesting an SSBI, the PSI be will complete without the information.

- a. True
- b. False

11. A DSS PSI may be released to a non-DoD agency by which one of the following?

- a. The activity security office
- b. The CAF
- c. The subject's supervisor
- d. DSS

12. The subject may obtain a copy of his/her PSI by requesting it from

- a. The supervisor
- b. The CAF
- c. The investigative agency
- d. The activity security office

- 13. Any person may review the personal information in a PSI.**
- a. True
 - b. False
- 14. The collection of personal information by the Federal government is governed by the _____.**
- 15. What are the five major SAPs within DoD?**
- a. _____
 - b. _____
 - c. _____
 - d. _____
 - e. _____
- 16. Who is responsible for SCI determinations on military personnel assigned to a Defense agency?**
- _____
- 17. _____ is the directive that governs SCI procedures for all personnel.**
- 18. What are the four steps in due process for military and civilian personnel?**
- a. _____
 - b. _____
 - c. _____
 - d. _____

19. Due process must be given to all of the following except:

- a. U.S. citizens
- b. Foreign Nationals
- c. Immigrant aliens

20. Which of the following best describes "due process"?

- a. The procedures used by a CAF to deny or revoke a security clearance or eligibility to be assigned to sensitive duties.
- b. The procedures used by an activity to deny an interim security clearance.
- c. The procedures used to deny or revoke an LAA for a foreign national employee.
- d. The procedures used by a CAF to determine a subject ineligible for military service.

21. Which of the following best describes an SOR?

- a. A letter notifying the subject that his/her security clearance has been revoked.
- b. A letter notifying the subject of a proposed action to deny or revoke his/her security clearance.
- c. A letter notifying the subject of the reasons for a proposed denial or revocation of security clearance or sensitive duty eligibility and the opportunity to reply.
- d. A letter notifying the command of a proposed denial or revocation of security clearance or sensitive duty eligibility for an assigned military member or civilian employee.

22. DOHA is responsible for denying or revoking the security clearance of a contractor employee.

a. True

b. False

23. If a CAF revokes a security clearance, the subject may _____ that decision to a higher level of authority.

Solutions & References

1. b. False (DoD 5200.2R, para 5-101)
2. b. Denying or revoking security clearance and sensitive duty eligibility. (Lesson 4, page 4-3)
3. b. False (DoD 5200.2R, para 7-101c)
4. c. PR (DoD 5200.2R, para 9-102a)
5. b. Disqualifying and mitigating conditions (Lesson 4, page 4-10)
6. d. Authorizing retention in military service or civilian employment.
(Lesson 4, pages 4-7/4-8)
7. b. Lessens the severity or seriousness of a disqualifying condition. (Lesson 4, page 4-10)
8. Bias or personal bias (Lesson 4, pages 4-13)
9. c. Subject (DoD 5200.2R, para 2-502)
10. b. False (DoD 5200.2R, para 5-105)
11. d. DSS (Lesson 4, page 4-23)
12. c. The investigative agency (Lesson 4, page 4-24)

13. b. False (Lesson 4, pages 4-21) (Must have a need to know)

14. Privacy Act. (Lesson 4, page 4-18)

15. (DoD 5200.2R, Chapter 3, Section 5)
 - a. SCI
 - b. SIOP-ESI
 - c. Presidential Support
 - d. Nuclear PRP
 - e. NATO

16. Appropriate Military Department CAF (DoD 5200.2R, Para 7-101 d.)

17. DCID 6/4 (Lesson 4, page 4-27)

18. (Lesson 4, pages 4-28)
 - a. CAF issues an SOR
 - b. Person may reply w/command position
 - c. Command position
 - d. CAF considers reply and command position
 - e. CAF makes final decision

19. b. Foreign Nationals (Lesson 4, page 4-32)

20. a. The procedures used by a CAF to deny or revoke a security clearance or eligibility to be assigned to sensitive duties. (Lesson 4, page 4-26)

21. c. A letter notifying the subject of the reasons for a proposed denial or revocation of security clearance or sensitive duty eligibility and the opportunity to reply. (Lesson 4, page 4-30)

22. b. true (Lesson 4, page 4-29)

23. appeal (Lesson 4, pages 4-28)

LESSON 5

ADJUDICATIVE ISSUES

In the previous lesson, we looked at the functions of a CAF and your responsibilities as an adjudicator to make personnel security determinations. This lesson deals with the process of how you determine when a PSI is ready for adjudication and how to evaluate the information for a determination. First, we will look at the elements of the adjudication process.

When reviewing a PSI, you must first determine if it is complete and ready for adjudication. If there are unresolved issues, then additional investigation will be necessary to obtain the information.

The next step is to determine what information is relevant to consider. Information that is directly related to evaluating allegiance, trustworthiness and reliability is relevant for personnel security purposes. Once the relevant information has been identified, you can then begin to evaluate the information and make a determination.

To aid you in making consistent determinations, a set of adjudication guidelines have been developed. They are divided into thirteen general categories of information that relate to a subject's allegiance, trustworthiness and reliability.

Each guideline is divided into disqualifying and mitigating conditions. A disqualifying condition is information that is serious enough by itself to be the basis for an unfavorable determination. A mitigating condition is information that reduces the severity or significance of the disqualifying condition. Sufficient mitigating conditions can permit a favorable determination to be made even though there are disqualifying conditions present.

The guidelines help you to evaluate the two general categories of information - allegiance issues and suitability issues.

This lesson contains examples of each of the adjudication guidelines and how disqualifying and mitigating conditions are evaluated. We will also look at the adjudication guidelines that involve allegiance issues. We will discuss the guidelines used in evaluating trustworthiness and reliability which are referred to as suitability issues. You will see several examples of where conditions from more than one guideline is involved. This interrelationship of conditions results in complex determinations and is present in many PSIs. After completing the lesson, you will better understand the decision making process involved in adjudications.

READING ASSIGNMENT

DoD 5200.2R Chapter 2: Sections 2, 3 and 4
DoD 5200.2R Chapter 6: all

Memo of Nov 98

IDENTIFYING ADJUDICATIVE ISSUES

Allegiance and suitability are the two general categories of information.

When you are reviewing a PSI or other information, you are looking for any relevant information that would raise a question about the subject's allegiance, trustworthiness or reliability. Allegiance and suitability are the two major categories of information that you will see. You must be able to determine what types of information could indicate an issue about the subject's allegiance or suitability.

Allegiance Issues

An allegiance issue is one wherein the subject's allegiance to the United States may be in question. This may be demonstrated through: support of unlawful means to overthrow the United States government; providing classified information to foreign countries; showing a preference for a foreign government over ours. The subject may also participate in or support activities that would deprive individuals of exercising their constitutional rights.

Suitability Issues

Suitability issues are all other types of information that may question a subject's trustworthiness or reliability for access to classified information or assignment to sensitive duties. These issues include: **criminal conduct; security violations; emotional, mental, and personality disorders; drug involvement, alcohol consumption; sexual behavior; financial considerations; misuse of information technology systems; outside activities; personal conduct; allegiance to the U.S.; foreign influence; foreign preference.**

Disqualifying and Mitigating Information

disqualifying and mitigating conditions.

As an adjudicator you must recognize the information in the PSI that may be serious enough to be disqualifying information is the basis for making adverse personnel security determination. This involves serious misconduct, improper or irresponsible behavior, or medical conditions which cast a doubt on the subject's allegiance, judgment, trustworthiness or reliability.

PSIs may also contain mitigating information. This type of information reduces the severity or significance of the disqualifying information. The mitigating information may be sufficient to overcome the disqualifying information and a favorable personnel security determination could be made. (Figure 5-1)

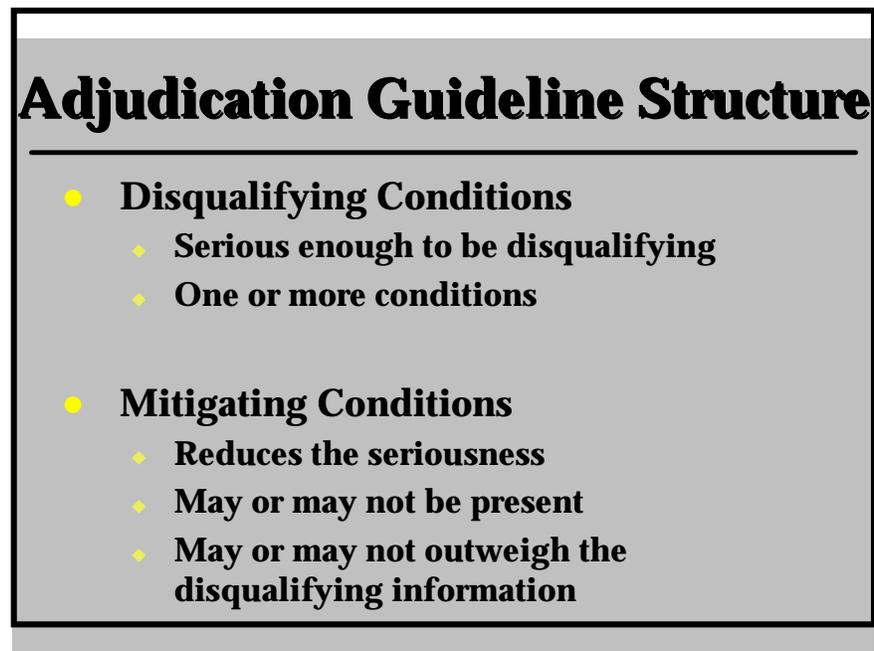


Figure 5-1

Adjudicative Process

First, you must determine if the PSI is complete and ready for adjudication. If there is an unresolved issue, then additional investigation may be necessary to obtain the information.

After reviewing and considering the relevant information, a determination must be made to make a favorable decision or start action to make an unfavorable decision.

IDENTIFYING ADJUDICATION ISSUES

How to identify issues.

There are both security criteria and adjudication guidelines provided in the DOD 5200.2R to aid you in determining the presence of issues and making determinations about the subject's allegiance, judgment, trustworthiness and reliability. The criteria are stated in paragraph 2-200 of the regulation. They are used to determine eligibility for clearance, access or assignment to sensitive duties.

Each criterion **identifies** a type of information that must be considered in the adjudicative process. The thirteen adjudication guidelines of Appendix I of the regulation are to aid you in **evaluating** the information.

Each adjudication guideline contains disqualifying and mitigating conditions for that type of information. The adjudication guidelines are the primary reference you will use to identify issues and make adjudications

DETERMINING THE RELEVANCE OF INFORMATION

Is the information directly related to the security issues?

Only information directly relevant to the personnel security standard may be considered in the adjudicative process. This involves both **favorable** and **unfavorable** information related to the security criteria and the adjudication guidelines. **Information must have a direct bearing on the criteria or guidelines to be relevant for adjudicative purposes.**

For example, the fact that a subject can only produce 50 items per hour instead of the 55 items per hour in the work performance standard has no bearing on his/her allegiance, judgment, trustworthiness or reliability. The fact that the subject may **falsify** his/her productivity records to meet the performance standard is relevant because it bears directly upon his/her trustworthiness.

All information provided for adjudication must be reviewed for its relevance before it is applied to the actual personnel security determination. Information provided by individuals, employers, official records, etc., may provide both relevant and irrelevant information for adjudication.

Whether factual or opinion, is it relevant?

The sources of information, especially individuals, providing facts, and in many cases, personal opinions that they think are important. Some of the information may be important and some will not be from an adjudicative viewpoint. This is a difficult part of adjudication, trying to sort out what is relevant and what is not.

You must not let your personal biases or other outside, non-adjudicative conditions influence your decision. This is to ensure that the adjudication reflects a proper application of the criteria and guidelines and is an equitable decision based solely on the merits of the security issues involved.

You are not concerned with the subject's work performance, community activities or the life-style **unless** there is a direct bearing on the allegiance, judgment, trustworthiness or reliability of the subject.

RESOLVING INCOMPLETE INFORMATION

Many times when issues are raised, the information is not complete enough for you to make a determination. In those cases, you must attempt to obtain the information needed so that a final determination can be made.

How to obtain complete information.

There are four means available to you to resolve an issue.

Re-opening PSIs

The first method is to re-open the PSI if the issue was raised but not fully resolved. Occasionally, PSIs conducted by DSS may have an unresolved issue. When this happens, return the PSI to DSS for re-opening to resolve the issue.

An example of this is the subject was convicted of drug possession and ordered to undergo a drug counseling program. The PSI did not get any record from the drug counseling program. The PSI should be re-opened to obtain the information.

Special Investigative Inquiry (SII)

The SII is used to gather information on specific issues that arise after the initial PSI or PR has been completed and adjudicated. For example, the subject had a favorably adjudicated SSBI a year ago. Information on an arrest by the local police arrives at the activity. The activity would request an SII from DSS for the details and disposition of the arrest. The CAF would make a determination based on the information in the SII. The CAF could use the information to revoke the security clearance.

ANACIs pose an unusual problem because OPM will complete the ANACI, but any expansion must be done by DSS. If an ANACI requires expansion, DSS will conduct an SII. This occurs most often with the situations shown in Figure 5-2.

- **Hostage situations**
- **Disposition of criminal offenses**
- **Derogatory comments from references**
- **Citizenship or naturalization information**

Re-opening the original PSI and the SII are two means of obtaining more information about an unresolved issue.

Medical Issues

If additional medical information is required, the CAF or the activity, depending upon Component procedures, may request a government physician to review medical information or offer a medical evaluation to the subject to obtain the current medical information.

For personnel security purposes, a medical evaluation cannot be required of a civilian employee, only offered. If the subject declines the offer, the adjudication must be based on the available information.

The subject may choose to have his/her personal physician provide medical information. The government physician should review that information and give a medical opinion as to whether the subject has a condition that may affect his/her judgment, trustworthiness, or reliability

Resolving Current Criminal or Counterintelligence Issues

If the information appears to involve a current counterintelligence (CI) issue or criminal conduct that might affect DoD, you should first go to the CI or criminal agency supporting the Component. If they determine there is no current CI or criminal interest, then the request could go to DSS. Examples of this are:

- **Willful compromises of classified information**
- **Foreign travel to designated countries**
- **Criminal activity on base**
- **Selling drugs to military personnel**
- **Committing crimes or conspiracy to commit crimes against the Federal government.**

Figure 5-3

Any of the types of information shown in Figure 5-3 should be initially referred to the CI or criminal agency unless the matter has already been referred. If a request is sent to DSS and current CI activity is indicated, DSS will stop the PSI and refer it to the proper agency. DSS will complete the PSI after the CI investigation is finished. If there is current criminal activity, DSS will complete the PSI except for the current criminal activity.

So far, we have recognized adjudicative issues in a PSI. If there were unresolved issues, we requested additional investigation to obtain the information. We have now identified the relevant information we will evaluate. The next step is how to evaluate the information.

EVALUATING FORMATION

How do you evaluate information?

The adjudication of information is an evaluation of information using nine conditions. These conditions are designed to help you evaluate both the positive and negative information about the subject. The end result of your evaluation is a decision whether the subject can be trusted to properly perform his/her duties. These conditions are shown in Figure 5-4. An explanation of them follows the figure.

EVALUATION CONDITIONS

- **Nature, extent, and seriousness of the conduct**
- **Circumstances surrounding the conduct, to include knowledgeable participation**
- **The frequency and recency of the conduct**
- **The individual's age and maturity at the time of the conduct**
- **The voluntariness of participation**

- **The presence or absence of rehabilitation and other pertinent behavioral changes**
- **The motivation for the conduct**
- **The potential for pressure, coercion, exploitation, or duress**
- **The likelihood of continuation or recurrence**

FIGURE 5-4

The **nature and seriousness of the conduct** refers to what type of conduct it is and how serious it is. It may vary from minor in nature, such as a traffic violation, to a major issue, such as an arrest for murder.

The **circumstances surrounding the conduct** refers to the contributing conditions that may have caused the conduct. The arrest for murder could have been the end result of the subject killing another person in a drug deal (illegal) or it was self-defense from a violent attack (legal). If the subject was with a group of people and did not know the incident took place and did not participate, then this would be in the subject's favor. The arrest is just the first official reaction to the conduct until a prosecutor or court can sort out the circumstances.

The **frequency and recency of the conduct** refers to how many times has the subject committed the conduct and when. A single offense that occurred ten years ago is of a different concern than five of the same offenses happening within the last four years.

The **age of the subject at the time of the conduct** will help to determine his/her **maturity**. Should the subject have known not to commit the conduct or was his/her immaturity a contributing condition? It is easier to understand the action of a naive seventeen year old who

lives at home than a thirty year old who has lived life on his/her own for years.

The **voluntariness of the participation** refers to how the subject was involved. Did he/she knowingly and intentionally participate? Was the subject unaware of what was happening until later on? Did the subject involuntarily participate because he/she was pressured or threatened if he/she did not become involved?

The **absence of presence of rehabilitation** refers to the subject's efforts to overcome a problem. What was his/her motivation to be rehabilitated? Did the subject voluntarily enter an alcohol rehabilitation program? Was the subject ordered into the rehabilitation program by a court? Did the subject successfully complete the rehabilitation or fail it and return to alcohol abuse?

The **motivation for the conduct** refers to the driving conditions behind the conduct. Did the subject commit the crime because he/she needed money to purchase drugs or alcohol? Was the individual coerced due to peer pressure or threatened.

The **potential for pressure, coercion, exploitation, or duress** refers to whether the individual is vulnerable because of something he or she has done. This could be drug involvement, mental or emotional problems or criminal activity that only a few people may know about and the subject is trying to keep quiet or hide.

The **likelihood of continuation or recurrence** refers to the passage of time. This means an incident has occurred so recent in time (less than one year) as to preclude a determination that recurrence is unlikely. Will it happen again?

The thirteen adjudication guidelines that follow, take these considerations into account in the disqualifying and mitigating conditions. You are looking at the conditions that could influence potentially disqualifying conduct. These considerations help to explain why the subject committed the conduct and is there reason to believe he/she may do it again?

Each of the following guidelines should be evaluated in the context of the whole person. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior.

However, notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, or adverse information.

When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

- **Voluntarily reported information**
- **Sought assistance & followed professional guidance**
- **Resolved or appears likely to favorably resolve the security concern**
- **Demonstrated positive changes in behavior and employment**
- **Should have access be temporarily suspended pending final adjudication**

Figure 5-5

If after evaluating information of security concerns, you (the adjudicator) decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future

incidents of a similar nature may result in revocation of access.

ALLEGIANCE ISSUES

Allegiance is the most important issue.

Allegiance questions are the most significant and potentially damaging issues to national security you will review. Allegiance issues go to the very foundations of our constitutional form of government.

This means the subject **may be or is** supporting the goals, objectives or policies of other governments, organizations, groups or individuals in preference to those of the United States. Those interests may be contrary to law or official United States policies. This includes the violent overthrow, attempted violent overthrow, or participation or support of any other unlawful means to overthrow the United States government or any state/local government.

A secondary aspect of an allegiance issue is that of the subject participating in or supporting organizations, groups or individuals that are involved in, advocate, or aid actions that would unlawfully interfere with an individual or group exercising their constitutional rights. Examples of this are preventing people from voting in elections, exercising the right of free speech and the right of lawful assembly.

Allegiance issues are covered by six of the criteria of paragraph 2-200 and three adjudication guidelines from Attachment 2 (Nov 98 Memo). Figure 5-6 shows the criteria and the adjudication guidelines that apply to them.

CRITERIA AND GUIDELINES ASSOCIATED WITH ALLEGIANCE

<u>Criteria Element</u>	<u>Adjudication Guideline</u>
Para 2-200a-d	Allegiance to the United States
Para 2-200e	Security Violations
Para 2-200f	Foreign Preference

FIGURE 5-6

***Read this
carefully!***

If a allegiance issue is present in a PSI or other information, three actions must be taken:

- Immediate referral to the CI agency to determine if there is a current or potential threat to the national security. The referral is made if the CI agency has not previously seen the information.
- The activity must determine whether to temporarily suspend access to classified information or performance of sensitive duties.
- Immediate referral to the CAF. In most cases, PSIs are usually routed to the CAF upon completion by the investigative agency and these actions would already have been started. If the PSI or other information is first received by the activity, the activity then must start these actions.

The remainder of the criteria and adjudicative guidelines deal with suitability issues that reflect on the subject's trustworthiness and reliability. **Suitability issues will be discussed later in this lesson.**

Review Assignment

Review the criteria of DoD 5200.2R, paragraphs 2-200a-f (page II-2) and the adjudication guidelines of Allegiance, Foreign Preference and Security Violations (NOV 98 MEMO). The two examples illustrate the types of allegiance information that you may see and the application of disqualifying and mitigating conditions.

Example 1

The employing activity requests a SSBI on a new civilian employee who will require a Top Secret clearance. The subject has a favorably completed NACI from employment with another Federal agency. The activity makes an emergency appointment to the critical-sensitive position and grants an interim Top Secret clearance.

A DSS Special Agent conducts a subject interview as a part of the SSBI. During the interview, the subject states that he was once the secretary of the New Free America Liberation Coalition. (This was not shown on the SF 86) The goal of this group was to overthrow the US government by any means, including violence, to establish a worker state. The subject claims that he supported the goals of the group as he understood them at the time. He only later found out that the group secretly advocated both unlawful and violent means to overthrow the U.S. government. The DSS agent then informs the activity and the PIC.

The CI agency of that Component would be immediately notified by DSS. As there appears to be a current CI issue and a possible threat to the US government, DSS would temporarily stop conducting the SSBI. The employing activity would notify the local CI agent that services the activity and notify the CAF of the information. At the same time, the employing activity decides to temporarily suspend access to classified information pending the outcome of the CI investigation, completion of the SSBI and the CAF action.

To this point, the activity has taken the proper actions to protect the national security by temporarily suspending access to classified information, notifying the CI agency and notifying the CAF.

Evaluation of Example 1

You are now reviewing the CI report and completed SSBI on the civilian employee. The CI agency report indicates the Department of Justice (DOJ) has no information about this group. When questioned by the CI agent, the subject stated that he had bragged to some of his friends in college that he belonged to this group, which in reality, did not exist. He told the DSS agent this because he was afraid DSS agents would talk to his friends and discover the subject's statements about the group; therefore, he had to make up a believable story to cover it. The subject stated that he believed in the U.S. constitution and form of government and would support it.

The problem for you is that there was initially a potential allegiance issue involved. Subsequent investigation indicated the subject was making up the story and got caught up in it when interviewed by the DSS agent.

No allegiance issue here, but a definite suitability question.

There is no real allegiance issue here; however, the subject's false statements to the agents question his suitability to be granted a security clearance. You were faced with a subject who created a false story and got caught up in it.

If the subject had actually belonged to this group and stated that he would take up arms to achieve the violent overthrow of the U.S. government, or support any other unlawful means, then there would be an allegiance issue. In that case, you would refer the case to a senior adjudicator for an allegiance review.

Mitigating Information in Example 1

To illustrate how the mitigating conditions affect allegiance issues, let's look at the civilian employee. We will add some new information to the example.

Presume the employee was 25 years old and graduated from college and this was his second federal job at the time of the interview. Presume the subject actually joined this group out of curiosity while attending college and he was 19 years old at the time. He belonged to it for a year and, for a short time, became the secretary of the group. He initially supported the concept of a worker state and thought it would come about through the election process because of the dissatisfaction of many citizens. Once he found out the group believed in using armed force and other unlawful measures to achieve a worker state, he left the group. This was confirmed through DSS interviews with other students.

The completed SSBI contains a full written statement about his current favorable beliefs in and intentions to support the United States government. The adjudicator must consider that the subject joined the group and supported the concept of a different form of government that would come about through popular support by lawful means (the election process.) This was a popular peer position during his time in college. At that time he was in his young adult years and was not aware of the unlawful and violent measures the group considered using. Once he found out about this, he left the group. It has been five years since his association with the group.

This case contains sufficient mitigating conditions to believe that the subject is not an allegiance concern and a favorable determination could be made.

Example 2

A military member currently holds a Secret clearance and has access to Secret information in the performance of his duties. One night, the local police arrest the military member in town for driving under the influence of alcohol. While taking the

military member into custody, the police officer observes an open envelope on the car seat. He takes the envelope into custody to record it with the military member's property at the police station.

When listing the contents of the envelope, the officer sees documents marked "SECRET" and a map indicating where the documents should be left. The officer contacts the military base and tells the investigators what he has found. The base investigator then notifies the CI agency of the situation. A CI agent takes custody of the military member and the documents at the police station.

The military member tells the agent that he was going to deliver the documents and pick up money for them. He had made a deal with a Russian intelligence agent to provide classified information about a weapons program he had access to. The base then suspends the military member's access to classified information and notifies the CAF.

To this point, the base has taken the necessary steps to suspend access to classified information, notified the CI agency, and the CAF of the situation.

Evaluation of Example 2

A textbook example of espionage.

You are now reviewing the case file of the military member. The file indicates the subject had a favorably completed ENTNAC. There was no other information in the file until the civilian police agency report was submitted by the base. The completed CI agency report indicates the military member was recruited to spy for the Russians. In this case, there is an allegiance issue involved. You would refer this case to a senior adjudicator for an allegiance review and possible removal from military service on allegiance grounds.

Mitigating Information in Example 2

The action of the military member is an example of espionage. The military member was recruited to sell classified information to the Russians. He was attempting to deliver the classified information for money when he was arrested on a traffic violation. There are no mitigating conditions in this example.

Receiving Allegiance Information

In both of the examples, the activity became aware of information that indicated a potential allegiance issue. The information came from different sources, one during a PSI and the other as a result of a civilian police agency report. In both cases, the activity was initially notified and started the necessary actions to protect classified information and reported it to the proper organizations

Recap

We have explained what types of information, disqualifying, mitigating, make up an allegiance issue. The examples illustrated what the activity and DSS do when first confronted with a potential allegiance issue. The first example also provided two different types of mitigating conditions. First, the mitigating conditions revealed that there was no allegiance issue. The other mitigating conditions reduced the significance of the disqualifying conditions. The second example provided a case of current espionage in which there were no mitigating conditions.

You will not see many actual allegiance cases; therefore, you must be careful not to overlook this type of information. When you see a potential allegiance issue, refer it to a senior adjudicator or supervisor for review.

SUITABILITY ISSUES

Suitability issues involve any behavior, condition, circumstances or other factors that directly affect the subject's trustworthiness or reliability. The security criteria

and adjudication guidelines will be discussed in the following sections.

Now, the rest of the story!

Each section will include disqualifying and mitigating conditions plus examples of how they are applied.

The last section will deal with a PSI involving disqualifying and mitigating conditions from several criteria and guidelines. Figure 5-7 identifies the adjudicative guidelines used to evaluate suitability information. conditions. The second example provided a case of current espionage in which there were no mitigating conditions.

You will not see many actual allegiance cases; therefore, you must be careful not to overlook this type of information. When you see a potential allegiance issue, refer it to a senior adjudicator or supervisor for review.

<u>CRITERIA</u>	<u>ADJUDICATION GUIDELINE</u>
NOV 98 MEMO	Foreign Influence
NOV 98 MEMO	Foreign Preference
NOV 98 MEMO	Allegiance to the U.S.
NOV 98 MEMO	Security Violations
NOV 98 MEMO	Criminal Conduct
NOV 98 MEMO	Emotional, Mental or Personality Disorders
NOV 98 MEMO	Misuse of Information Technology Systems
NOV 98 MEMO	Financial Considerations
NOV 98 MEMO	Alcohol Consumption
NOV 98 MEMO	Drug Involvement
NOV 98 MEMO	Personal Conduct
NOV 98 MEMO	Outside Activities
NOV 98 MEMO	Sexual Behavior

Figure 5-7

Note: Paragraph 2-200i is a general criterion. It is used when a subject's acts, or lack of them, reflect on his/her trustworthiness or reliability and the conduct does not fit into any of the adjudication guidelines. This does not happen often as the guidelines cover mostly all conduct that could impact on a subject's trustworthiness or reliability.

SECURITY VIOLATIONS

Does the subject follow security regulations or show a disregard for them?

This guideline looks at how the subject follows laws, Executive Orders and regulations involving the protection of classified information and other established security procedures necessary to protect information, personnel and property. **Non-compliance with security regulations raises doubt about an individual's trustworthiness, willingness and ability to safeguard classified information.**

A subject who violates security procedures, intentionally or accidentally, can pose a risk to the protected information, personnel or property. He/she could cause the loss or compromise of classified information to persons who are not authorized to receive it. Violation of security procedures can cause varying degrees of damage to the national security.

A minor violation could be a safe left open (administrative violation with no compromise) which costs manpower to investigate the violation and time to correct the problem and discipline the subject.

A major violation could be a loss of military advantage (a new weapons system) costing both an advantage in wartime, plus development costs up to billions of dollars for some advanced major systems.

Types of Security Violations

Security violations are deliberate or inadvertent.

Violations of security responsibilities can be either inadvertent or deliberate. This may be to sell property or information for his/her own monetary benefit. Information could be sold to a foreign government or persons (then it becomes an allegiance issue) or to a contractor seeking a contract or proprietary information (information belonging to a private firm but the government has a legal or contractual interest in it) to further his/her company. Also, it could be

the destruction of documents to reduce the subject's workload or accountability of documents. The subject may provide information to someone else to further his/her position.

This practice is known as "**leaking**" and usually involves classified or sensitive information. The purpose is usually to cause others to agree with his/her position when there may be opposition to it at the subject's level or at higher decision-making levels. Information that is "leaked" may end up in the news media with persons without official authorization to see it or to Congress for political purposes.

A subject who accidentally, or negligently, discloses classified information can also cause damage to the national security. If the information is lost or compromised through improper handling, mailing, or accountability, time will be lost to investigate and correct the situation.

If the information falls into the hands of people not authorized to receive it, the compromise can have varying degrees of damage. The damage could vary from just one person seeing it, turning it over to a foreign government or to the news media, or others using it for their own purposes.

Any of these circumstances would damage both our national security and the public's perception of our ability to properly safeguard our secrets.

Review Assignment

Review paragraph 2-200g (page II-2) and the guideline for Security Violations, (Nov 98 Memo) before reading the examples. The two examples illustrate types of information you will see involving this condition and how the adjudicative guideline is applied.

A lack of security training contributed to this problem.

Example 1

The subject frequently traveled to meetings throughout the country on a new weapons project. The weapons project is classified and all of the documents about it are classified. The subject carried the documents with her on the airplane each time she went to one of the quickly called meetings. During the next security briefing, the procedures for hand carrying classified information were discussed. The subject reported to the speaker that she had carried classified documents on three trips.

An investigation was conducted by the security office. The investigation revealed the subject had **never received any type of security briefing or training** on how to handle classified documents. The supervisor had merely told the subject to "be careful with that stuff."

On one hand, carrying the classified documents without authorization on three separate occasions is a disqualifying condition. On the other hand, the subject had never been instructed on how to properly handle the classified information.

In good faith, she took the supervisor's instructions, "to be careful with that stuff," as the way to handle it. This is a strong mitigating condition as the subject was not properly trained in how to safeguard the classified documents, so it is difficult to hold her solely responsible for the improper handling.

If the subject had received proper security training and still hand carried the classified information without authorization, then it would have been an intentional violation of security regulations with no mitigating conditions.

In this case, there is a valid mitigating condition to consider in the adjudication and it would support a favorable decision.

Example 2

On four separate occasions, the subject has been reported for leaving his safe open after duty hours. Each time the safe was found open by the guard force during an office check after hours. When interviewed by the security office about the latest violation, the subject stated he didn't think the procedures were necessary as the information shouldn't be classified and he would lock up the safe if he remembered to do so.

This subject just doesn't care about protecting classified information.

In this case, the subject had received the proper training on securing classified information at the work site and had received supervisory reprimands for the previous violations. He disagreed with the document classification, but still had an obligation to properly protect it. He indicates the safe may be properly secured if he remembers to do so.

This statement, considered along with the previous violations, is not a positive indication that the subject intends to comply with security directives.

There are no mitigating conditions in this case; therefore, the decision would be unfavorable.

CRIMINAL CONDUCT

This guideline involves **any criminal conduct regardless of whether or not the person was formally charged**. The conduct includes violation of any Federal, state or local county/municipal law, or the laws of foreign countries.

Look for intent in criminal conduct.

A subject who violates laws raises questions about his/her trustworthiness and reliability. Criminal conduct can range from a minor traffic violation to serious offenses such as murder and espionage. The more serious the offense, or a pattern of criminal conduct, the more the subject's trustworthiness and reliability are doubted.

A subject who intentionally commits a crime is more of a security concern than a subject who accidentally commits an offense such as a traffic violation. **The difference is in the intent of the subject to do something.** If the subject knowingly and intentionally commits a crime, what reliance can we place in the subject to properly safeguard classified information or perform other sensitive duties? He/she has either demonstrated an intent to disobey or has already deliberately disobeyed laws. What will the subject do if he/she does not respect or agree with security or other regulations?

We cannot afford to take the risk to national security with this type of subject. This individual demonstrated willingness to place himself, or herself, above the established laws of the community as they personally see fit. **This creates a doubt about his/her trustworthiness and reliability.**

Evaluating Criminal Conduct Information

When evaluating information about criminal conduct, you must consider all available information about the criminal conduct, both good and bad. **Remember, you are making a personnel security determination, not conducting a criminal trial of the subject.** Even though a subject may have had criminal charges dropped, or had not been charged, it only means there may be no further criminal prosecution of the subject. There may still be valid personnel security concerns if the subject engaged in criminal activity, but for some reason was not convicted.

You are concerned about the subject's intent and actions in any criminal conduct. For example, the subject may show a willingness to assault people with no apparent reason and cause serious injury. From a personnel security viewpoint, this conduct raises questions about his/her trustworthiness and exercise of responsible judgment. He/she may not be convicted of assault because the subject threatened the victims with more violence if they prosecuted him/her, so the victims will not say anything. This does not reduce the

Don't dismiss the significance of the information just because the subject

was not convicted.

significance of the information about criminal conduct. In this case, the subject intended to harm others without any lawful reason, such as self-defense from attack, and threatened the victims if they acted against him/her. **Is this a person we could trust with our secrets?** When mitigating conditions are present, a favorable decision is possible in many cases. Many people who commit a crime only do it once. The emotional impact of the crime and the decision of the judicial system can cause the subject to change his/her way of thinking about committing crimes. **This is one reason that the passage of time, or recency, can be a mitigating condition.** This lets the subject prove him or herself by personal conduct over a period of time. We cannot take his/her word immediately because the subject may lie about not committing crimes again and some subjects do not know in their own minds what they will do for awhile.

Time is an important mitigator.

The time period gives the government the opportunity to see how the subject will conduct him or herself after the crime. In most cases, the subject does not commit any further crimes. These subjects may later become eligible to be granted security clearances or perform sensitive duties. In a few cases, however, some people just continue committing crimes. These are the few who remain security problems as they have shown a history of untrustworthiness and unreliability.

Review Assignment

Review paragraph 2-200h (page II-2) and the adjudication guideline for Criminal Conduct (NOV 98 MEMO) before reading the examples. The four examples show the types of information that you will see and how disqualifying and mitigating conditions are applied.

Example 1

An individual is selected for a noncritical-sensitive civilian position as a cashier at a base finance office. The application states there has been no criminal conduct on the subject's part and the local records check is favorable.

Based on this information, the activity makes an emergency appointment to the position and the subject goes to work.

When the ANACI is received at the base, it contains a record from a police department in another state which indicates that the subject was convicted of embezzlement from her employer. The record shows the subject is still on probation for another two years. In this example, the subject falsified the application by not admitting the conviction for embezzlement and the current probation. The subject hid this information so the employer would not find out. Because of this, the base decides to remove the subject from the job.

If a personnel security determination had been made, the decision would have been to declare the subject ineligible to perform sensitive duties. The personnel security issues are that the subject was convicted of embezzlement, is still on probation (so we do not know if subject will successfully complete it), and the subject falsified the employment application. **There are no mitigating conditions in this example.**

Example 2

An individual has been selected for a noncritical-sensitive civilian position requiring a Secret security clearance. On the application forms, the subject lists two convictions in 1991 and 1992 for assault and battery on his spouse.

When the ANACI is received at the activity, the two convictions are confirmed in the ANACI. The subject tells the activity security office that he completed a rehabilitation program in 1993. Since the ANACI does not contain the court records, the activity requests DSS to conduct an SII to obtain the court records. Upon receipt of the SII, the court records indicate the subject voluntarily entered a counseling program in 1992 and successfully completed it in 1993. The subject recognized that he had a problem dealing with the recent death of two daughters in a house fire. This was causing a family situation with the spouse so he sought the help. The

court took the subject off probation early due to the successful completion of the counseling. The SII shows no further criminal conduct. A favorable employment determination was made. A CAF adjudication was then requested.

In this example, the subject admitted to the criminal conduct on the application forms. The SII shows the subject took a positive step in recognizing that he had a problem because of the death of his daughters and sought help for it. There has been no criminal conduct since the last offense in 1992. The subject appears to have solved the problem he had and does not present a security issue at this time. **There is sufficient mitigating information in the example to make a favorable decision.**

Example 3

An individual is selected for a critical-sensitive civilian position requiring a Top Secret clearance. The subject admits on the SF 86 that she has been arrested three times for shoplifting but was convicted only one time.

The activity submits the SSBI request but does not make an emergency appointment. The subject is informed that she will be notified when the SSBI is completed and adjudicated. When the SSBI is received at the activity, it shows the subject has been arrested 22 times between 1972 and the present for charges of shoplifting, petty theft, unemployment fraud, auto theft and probation violation. She was convicted 14 times, all misdemeanor convictions, and placed on probation each time.

In the subject interview of the SSBI, the subject says that she did commit all the offenses listed even though several did not have a conviction. The subject lied on the application because she thought she would not get the job if the arrest information was listed on the application. **The activity informs the subject that she will not be appointed to the job.**

The personnel security issues in this example involve a pattern of criminal conduct and falsifying the SF 86. Because of the lengthy and current pattern of criminal conduct,

including violating probation, mitigating conditions probably could not overcome the disqualifying conditions in the case. **The pattern of continuous criminal conduct without any evidence of rehabilitation makes her trustworthiness and reliability too questionable for a favorable determination at this time.**

Example 4

A military member with a Secret clearance is currently stationed overseas. The subject's unit receives a report from the local police that the subject has been arrested for selling cocaine off base. The unit temporarily suspends the subject's access to classified information, notifies him in writing, and reports it to the CAF. The police report states the subject sold cocaine (tested positive by the police laboratory) to an undercover officer on two occasions. The two sales were recorded on videotape. The subject is not prosecuted because of a legal error.

In this example, the subject has violated foreign law by selling cocaine. Even though the subject was not prosecuted by the foreign government due to a legal error, the police information is sufficient to start an action to revoke the security clearance. There has not been enough time since the offenses occurred to determine if the subject may commit future criminal acts. **There are no mitigating conditions in this example.**

Complexity of Criminal Conduct Information

Criminal conduct is a difficult area of adjudication because of the variety of disqualifying and mitigating conditions that can arise. The four examples provided no mitigation, insufficient mitigation, or sufficient mitigation to affect the final decision favorably or unfavorably.

An important mitigating condition to consider is the long-term conduct of the subject. A period of time free from criminal conduct is more likely to indicate the subject has changed his/her attitude towards crime, but not always.

A pattern of criminal conduct is one of the best indicators

***Is the subject remorseful?
Will he/she commit crimes in the future?***

of a potential problem. Here the subject has demonstrated the criminal conduct over a period of time and there is a greater likelihood that there will not be sufficient mitigating conditions to make a favorable determination.

When reviewing police reports or statements to special agents, look for the subject's explanations and any signs that the subject is sorry for what he/she did. Also, look for any statement that the subject may commit further crimes. This occurs in drug abuse cases where the subject indicates he/she will continue to use drugs in the future but not at the job site. Using any illegal drug is still a criminal offense and the subject's declaration shows he/she intends to commit criminal acts in the future.

This alone is a sufficient basis to make an unfavorable determination. A statement of intent to commit future criminal acts casts a doubt on the subject's trustworthiness and reliability.

EMOTIONAL, MENTAL AND PERSONALITY DISORDERS

This guideline involves emotional, mental and personality disorders that can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability or stability.

Emotional, mental and personality disorders and illness may be severe enough that the individual cannot control his/her actions or make rational decisions.

Emotional, mental and personality disorders and illnesses can cause an individual to think and react differently than he/she normally would. The effects can be minor or major in nature and can be short or long-term in duration. The condition may be so serious that the individual's judgment and reliability may be impaired to such a degree that normal, rational decisions cannot be made. If this happens, or the possibility exists, then the individual must not have access to classified information or perform sensitive duties until he/she is no longer affected by the condition or until the possibility is remote that the condition will affect the individual's judgment or reliability.

Figure 5-8 shows some of the reasons for emotional, mental and personality disorders.

- An inherited condition
- Accident or injury
- Illness
- Degenerative disease
- Chemical imbalance in the body
- Effects of drug or alcohol abuse

Figure 5-8

Obtaining Medical Information

disqualifying conditions indicate this individual has a disorder that could result in a defect in psychological, social or occupational functioning. When information in a PSI indicates a potential problem area involving mental or emotional conditions, a credentialed mental health professional, acceptable to or approved by the government, should be consulted so that potentially disqualifying and mitigating information may be fully and properly evaluated..

Ask the medical professional for a medical opinion, not a security opinion.

For personnel security purposes, a medical examination cannot be required, it may only be offered to the subject. The medical professional should be given access to the PSI to review the information. The medical professional may be able to provide an opinion based on that information, or he/she may request the subject undergo a medical examination.

When a medical opinion is requested, the questions should cover any diagnosis and prognosis of a medical condition, if any, and whether the condition could cause a defect in the individual's judgment or reliability. **Do not ask the medical professional if the subject should have a security clearance.** He/she is a medical specialist, not a

personnel security specialist. He/she will not know all the requirements of the PSP.

By asking the medical professional for an opinion on whether the subject may have a condition that could affect the judgment or reliability, you can make a determination based on medical information rather than personal opinion.

If the subject declines the offer of a medical examination, the adjudication must be based on all the available information.

Review Assignment

In 2R review paragraph 2-200j (page II-2) and the adjudication guideline for Emotional, Mental and Personality disorders (NOV 98 MEMO) before reading the examples. The two examples show you what type of information you may see involving this guideline and how the disqualifying and mitigating conditions are applied.

Example 1

An individual begins acting violently at work. On two occasions, he assaults other employees. A medical examination for employment is conducted by the activity.

The diagnosis reveals the subject has developed a chemical imbalance, which causes mood swings. The condition can be effectively treated with medicines and the subject will not suffer any negative effects of the condition while taking the medicine.

The security office requests that the physician give a medical opinion of whether the condition could cause a defect in the subject's judgment or reliability. The physician states there should not be any problem with the subject's judgment or reliability if he continues to take the prescribed medicines.

The subject decides he doesn't like to take the medicines and sometimes does not take them. This occasionally

causes a problem at the work site with the subject becoming argumentative and hostile towards his co-workers and supervisors. The subject is sent to the activity physician for another medical examination for employment. The physician states the subject is not taking the medicines as prescribed. This action is causing the hostility observed at work and it will affect his judgment if the medicines are not taken for periods of time.

In this example, the subject developed a condition which affected his judgment and reliability, but which could be controlled with prescribed medicines. If the subject had continued to take the medicines as prescribed, the medical opinion indicated the condition would not cause a defect in the judgment or reliability. There was a disqualifying condition (the condition that could cause the defect in judgment or reliability). The subject refused to use the medicines as prescribed and it adversely affected his behavior and judgment.

As long as the subject refuses to take the medicines, he has a condition that would make him ineligible to have access to classified information or perform sensitive duties. If, at a later time, the subject decides to continue using the medicines as prescribed, then he may be eligible for access or sensitive duties. In mental or emotional disorders, the condition and its effects can change because of many conditions.

Sometimes the subject's own actions can help or worsen the conditions.

This example shows a situation where the subject had a controllable condition and would have been eligible, but through his own actions, he did not follow medical advice rendering himself ineligible at the time.

Example 2

An individual is selected for a noncritical-sensitive position requiring a Secret security clearance. The application indicates that she was hospitalized for one year due to episodes of paranoia, including violent conduct. The activity does not make an emergency appointment and advises the subject they will notify her when the PSI is completed.

The CAF then receives the ANACI but it does not contain any information about the hospitalization. The CAF requests DSS to conduct an SII to get information from the hospital. The completed SII contains a medical report that indicates the subject has a form of paranoia that manifests itself by violent conduct. There is a high probability of recurrence and when it happens, the subject cannot tell reality from fantasy and is not in control of her actions. Medication may not control the more serious incidents and the subject would have to be hospitalized. The activity does not hire the person as she could not properly perform the job duties and would cause a potential danger to other employees.

From a personnel security aspect, the medical report provides sufficient information to decide that there is a condition which will cause a defect in the subject's judgment and reliability. There is a high probability of recurrence and the medication could not adequately control the condition at all times. **There is not sufficient mitigating information in the example to make a favorable determination.**

Another Viewpoint

In reviewing information dealing with emotional, mental and personality disorders, you are faced with conditions that are, in many cases, beyond the subject's control to do anything about it.

It may not be the subject's fault, but it is still a security concern.

In some cases, the subject may contribute to the conditions that are causing the problem. When mental or emotional disorders are present, the subject may not be eligible for access or sensitive duties because he/she might not be capable of properly performing the duties, rather than because of some voluntary action on the part of the subject.

FOREIGN INFLUENCE

This adjudicative guideline involves situations where a security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence or obligation are:

- (1) not citizens of the United States or**
- (2) may be subject to duress.**

These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

disqualifying conditions increase the subject's vulnerability to coercion, exploitation, or pressure because of the attempt to hide those conditions or to protect relatives, friends or associates in foreign countries from any action taken against them to pressure the subject. Some subjects will go to great lengths to hide something about themselves or to protect others. In some of the worst cases, the subject could be blackmailed into providing classified information or performing the sensitive duties improperly.

Review Assignment

Review paragraph 2-200k (page II-2) and the guideline for Foreign Influence (NOV 98 MEMO) before reading the examples. The two examples show you the types of information you will see involving this guideline and how the disqualifying and mitigating conditions are applied.

Example 1

An individual is a naturalized United States citizen from Iran. The subject's immediate family (father, mother and two sisters) is still in Iran. The subject was selected for a

position requiring a Top Secret clearance. When the NAC portion of the SSBI was completed, the activity made an emergency appointment to the position, but did not issue the interim clearance as there were questions about a potential hostage situation.

During the subject interview portion of the SSBI in 1995, the subject stated that he had not divulged his association with the United States government to the family members in Iran during their correspondence. He also stated that he could not be pressured into providing any information or other assistance to Iran as he hated the current government and did not believe in it. The completed SSBI further developed information that the subject has made four trips to Iran: one in 1986; two in 1990; one in 1994. The subject did not report any of these trips on the SF 86, to the supervisor, or the security office.

These were potential CI issues; therefore, the subject was questioned by a CI agent. **The subject admitted that threats had been made against his family by officials of the current government.** If he did not cooperate and provide certain information when he went to work in the position, the family members would be executed. The subject stated that he was going to report this threat to the security office but had not done so. The subject requested a polygraph examination to confirm this. The polygraph examination was inconclusive on whether he told the relatives about his job and access to classified information. Since there was no further CI action to be taken, the CI case was closed.

A classic hostage situation.

The issues in this example show the subject had lied on the SF 86 by concealing the travel and not reporting the pressure applied against him by the Iranians (a hostage situation). The subject was vulnerable to pressure and there is a question of whether he would have reported it and possibly given the information to Iran.

In this example, there is doubt about the subject because he concealed information about the foreign travel and the attempted pressure by the Iranian government. There is a question of whether he may later give information to the

Iranians and it is not clear how the Iranians knew about his job duties. **There is too much disqualifying information to be overcome by the few mitigating conditions. In this example, the determination would be unfavorable.**

Example 2

An individual was selected for a noncritical-sensitive position, the ANACI requested, an emergency appointment made and an interim Secret clearance granted. On the SF 171 for the position, **the subject claimed a Bachelor of Science degree in electrical engineering and that she also held a state license to practice as an electrical engineer in New York.**

The position required the employee to possess at least a Bachelor of Science degree in electrical engineering from an accredited university/college and a New York State engineering license to meet the qualifications. When the completed ANACI was received at the activity, it indicated the subject had only 30 hours of credit at the university and no record of the New York State license.

The subject was questioned by the personnel office about her qualifications for the position. **The subject admitted that she lied** about the degree and the state license in order to get the job. She did not think the government would check the qualifications that closely as her previous employers had not checked them thoroughly.

During the interview, the subject admitted she had been pressured on another job to provide information. If she had not provided the information, the person would inform her employer of the false qualifications. That could get her fired and she did not want that, therefore, she resigned.

The subject was discharged during the probationary period and the final appointment to the position was not made because she lacked the necessary qualifications and falsified her application. From the personnel security aspect, this example brings out the issue of making false

There are many ways to pressure people to get them to do

something.

claims about qualifications in order to obtain a position and vulnerability to blackmail or pressure.

Not only did the subject attempt to get the job by lying about the qualifications, her statement to the personnel office about previous employers not closely checking the qualifications and the threat of pressure indicate a pattern of deceit. **This example contains no mitigating information.**

FINANCIAL CONSIDERATIONS

This adjudicative guideline involves excessive debts, continuing financial problems and unexplained change in lifestyle or increased income.

A subject's financial history can tell a great deal about how he/she handles responsibility. An individual who mismanages money, shows an indifferent attitude toward paying his/her debts, has a lifestyle well above what he/she can apparently afford or uses deception, including criminal acts to obtain credit, is someone who requires close scrutiny when making a personnel security determination.

Much of the information an adjudicator needs is contained in credit reports, subject interviews, and other financial records included in several of the PSIs. In the PSIs that do not include financial information as a normal part of the investigation, an SII can be conducted to obtain financial information if there is an indication of financial problems.

One reason so much emphasis is placed on finances is that money has figured as an important, if not the primary, factor in many espionage cases. The subject has either needed money to take care of his/her debts or just wanted more money to raise his/her lifestyle.

Reviewing Financial Information

When reviewing financial information, **you are looking for conduct, or a stated intent, by the subject** that describes both the financial picture and his/her attitude. Is the subject

someone who is reckless with spending money and shows an unwillingness to pay his/her debts? Or, is the subject someone who spends within his/her means, takes care of debts, or is making good-faith efforts to do so? A subject who is irresponsible in his/her financial dealings raises questions about his/her trustworthiness and reliability. Not everyone with financial problems who performs sensitive duties will become a spy; however, we cannot take the risk when trustworthiness and reliability are in question.

Review Assignment

In 2R review paragraph 2-2001 (page II-3) and the adjudication guideline for Financial Considerations (NOV 98 MEMO) before reading the examples. The three examples will show you the types of information you will see and how disqualifying and mitigating conditions are applied.

Example 1

A newly assigned junior enlisted military member is undergoing a SSBI for a Top Secret clearance for his new duties. When the completed SSBI is reviewed at the CAF, the credit report indicates that five accounts, totaling \$11,400, are more than 120 days overdue and two accounts, totaling \$3,600, have been sent for collection.

In the subject's statement, he said that he bought a car, a computer and several pieces of electronic equipment. He bought most of the items on impulse and received "instant credit" available at the stores. The subject stated he can not make all of the payments on the items. The car has just been repossessed. The subject stated he has not made payments on some of the items as he is not satisfied with them and probably won't make any further payments on those items.

The subject stated he attempted to obtain a loan from the credit union but was turned down due to his credit rating. **On the day before the interview**, the subject stated he purchased a \$1,500 stereo system with "instant credit" available at the store and will probably buy other things if he likes them.

In this example, the subject has demonstrated a lack of financial responsibility through impulse buying beyond his means to pay and states an intent to buy more.

The subject can not pay for the items already purchased and shows an indifferent attitude about paying for some of the items because he doesn't like them. This situation has already resulted in the repossession of the car.

With the stated attitude of not paying, creditors will be forced to repossess the items and, in some cases, may need court judgments against the subject to collect. **This example contains no mitigating information.** The subject appears headed for even more financial problems due to irresponsible spending and a negative attitude about taking care of his debts. **The decision in this example would be unfavorable.**

Example 2

An employee occupies a noncritical-sensitive position with a Secret clearance. **The employee asks the supervisor for some time off from work to go to court and petition for bankruptcy.**

Under the continuous evaluation program, the supervisor reports this information to the security office. The security office requests DSS to conduct an SII for financial information. **The completed SII reveals the subject filed for bankruptcy due to a business failure.** The subject is a machinist and had set up a business to make fittings and gaskets for oil-well drilling machinery. She had borrowed \$200,000 to set up the business with the necessary machinery. She had just received a contract for fittings and gaskets. At that time, the oil industry suffered a downturn and the contract was canceled. As the oil-well drilling equipment was not used due to a reduction in oil consumption, the bank had to repossess the equipment. The bank could not sell all of the equipment and took a loss. The remainder of the loan, \$140,000, had to be paid by the subject. The subject's current expenses already took most of her take home pay and she could not repay the remainder of the loan. The court arranged for a payment schedule to repay the loan and the subject was meeting the payment

schedule.

In this example, **the subject suffered a business related loss of income beyond her control.** Until that time, there had been no problems with the subject's financial status as she was handling the bills and other debts. The court approved repayment schedule was being followed by the subject. Her responsible actions to take care of the debts show a favorable attitude in taking care of financial obligations. **There is sufficient mitigating information in this example to make a favorable determination.**

Example 3

An employee occupies a noncritical-sensitive position but does not need a security clearance. The employee's annual salary is \$23,000. Until recently, the employee drove an older model car, wore casual clothes and lived a moderate lifestyle.

Recently, the subject started driving a new, expensive sports car, wearing custom-tailored clothes and was living a very high lifestyle. One of the co-workers reported this to the security office as **unexplained affluence.** The security office requested DSS to conduct an SII to determine the source of the subject's new affluence. The completed SII contained a statement that the subject had just won the state lottery prize of \$3,500,000. **This was confirmed by an interview with a state lottery official.**

In this example, the sudden change in lifestyle and affluence was a proper area to question as there was no apparent or known reason for it. The SII provided the mitigating information about the subject winning the lottery. This can happen when a subject receives an inheritance. The information explains the change in the subject's lifestyle and indicates there is no security issue here. **This example warrants a favorable determination.**

Overall Evaluation

The subject's and actions are important.

The three examples above describe different types of ***attitude*** disqualifying and mitigating information that may be contained in PSIs. Both the financial information and the statements are good indicators of the subject's attitude and actions in taking care of their financial responsibilities.

If the overall actions and attitude are favorable, there probably is not a security concern. If the overall attitude and actions are unfavorable, there will be a security concern about the subject's suitability to be granted a security clearance or perform sensitive duties.

ALCOHOL CONSUMPTION

This adjudicative guideline involves the occasional or continuing use of alcohol to excess. You are looking at how the use of alcohol affects the subject's trustworthiness and reliability.

Alcohol can cause a change in the subject's behavior to such a degree that he/she may be incapable of properly protecting classified information or performing sensitive duties. The ability to make responsible judgments and decisions is reduced and it contributes to irresponsible and sometimes criminal conduct. The use of alcohol frequently causes conduct or medical conditions which are related to other adjudication guidelines. **The misuse of alcohol is usually detected by the subject's conduct or medical problems.**

Review Assignment

In 2R review paragraph 2-200m (page II-3) and the adjudication guideline involving Alcohol Consumption (NOV 98 MEMO) before reading the examples. The two examples show the types of information you will see in alcohol cases and how the disqualifying and mitigating conditions are applied.

Example 1

A SSBI is being conducted on a military member to perform ADP-I duties but no security clearance is required. During the interview by a DSS agent, the subject states that he has been arrested three times for Driving While Intoxicated (DWI). The arrests all occurred between four and six years ago. A civilian court directed the subject to attend an alcohol program as a result of the last conviction for DWI.

The subject also voluntarily entered a military alcohol rehabilitation program at the same time. The subject successfully completed both the civilian and military programs and has not had any alcohol to drink since the last conviction. The SSBI also includes verification of successful completion of both programs and the local agency checks do not show any arrests or detentions since the last DWI arrest.

In this example, there is disqualifying information but there is also strong mitigating information. The successful completion of the two programs (one which the subject voluntarily entered), no further use of alcohol, and no record of any subsequent alcohol related conduct for the past four years are sufficient factors to overcome the disqualifying information. **The determination in this example is favorable.**

Example 2

Alcohol abuse affects the subject's judgment and may lead to unusual behavior.

An individual is employed in a critical-sensitive position with a Top Secret clearance. One day a police officer arrives at the activity with two warrants for the subject's arrest. The warrants are for Assault and Battery on his spouse and Leaving the Scene of an Injury Accident (Felony). The police officer tells the security office that the subject had been drinking when he assaulted his spouse. When the police arrived, the subject drove off and later was involved in an accident but was not arrested because he had left the scene prior to the police's arrival.

As this appears to be a serious situation with alcohol involvement, the security office suspends the access to

classified information and notifies the subject in writing of the suspension,

The activity requests DSS to conduct an SII to obtain any information about the subject's use of alcohol or criminal conduct. The completed SII is being reviewed at the CAF. The SII discloses the subject has two previous arrests and convictions. Both are alcohol related; one involving assaulting his spouse and the other a DWI within the last three years.

A subject interview also reveals that he attended a court ordered alcohol program after the DWI conviction, but the record shows that he **did not complete the program** as required. The SII also includes the court records for the latest two offenses. The subject was found guilty of assault and battery and leaving the scene of an accident. The second charge resulted in a felony conviction and the court ordered three years probation and successful completion of an alcohol program. The court records indicate subject had been drinking heavily at the time the incidents occurred but **the subject claimed he did not remember anything about the incidents.**

In this example, there is the following disqualifying information:

- The subject had two previous incidents involving alcohol which resulted in criminal convictions.
- The subject failed to comply with court orders to complete an alcohol program as a result of the criminal conviction.
- The subject was involved in two recent incidents, one resulted in a felony conviction - both were alcohol related.
- The subject is on probation for three years and must complete a court ordered alcohol program.
- The subject claims he does not remember the latest two incidents while drinking.

This information is recent and it questions the subject's reliability and trustworthiness.

He has repeated alcohol related conduct, the latest resulting in a felony criminal conviction. The subject may also have a medical problem due to alcohol as he cannot remember the incidents. The outcome of the probationary period and second court ordered alcohol program could be mitigating conditions after they are both successfully completed, but it is too early to make any decisions on that.

This example contains considerable disqualifying information and no real mitigating conditions. The determination at this time must be unfavorable. This information became known between the time the SSBI was completed and the PR was due. The PR would have picked up this information but the subject would have access to classified information for that period of time and could pose a risk because of the affects of alcohol. **This is an example of why the SII is used any time derogatory information is developed, even though there may be the requirement for a PR.**

The two examples show that alcohol related information may come from various sources, not just PSIs. Because of the frequent nature of alcohol related conduct and the many non-DOD sources of information, you normally must use the SII to obtain full information.

DRUG INVOLVEMENT

This adjudicative guideline involves the use, possession, sale, transfer or addiction to illegal drugs and other psychoactive substances. The use of these substances can have various effects on the subject's judgment, reliability, physical and mental health. The possession, sale, transfer and trafficking of these substances are illegal and, in many cases, are felony crimes. Involvement with drugs is frequently encountered in PSIs and other reports.

Evaluating Drug Involvement Information

Drug involvement is a voluntary action by the subject.

When considering any type of disqualifying information about drug involvement, keep in mind that the subject is intentionally involved in the vast majority of cases. Only if the subject is given drugs without his/her knowledge or if someone uses an unwitting subject to transfer drugs, would the subject not have a knowing participation. The mere use, possession, or other involvement with illegal drugs is a violation of Federal law, even if a state or local government were to decriminalize it.

There are certain exceptions to the Federal laws (such as use of marijuana for medical research or processing of cocaine for medical use), but these have official approval.

Mitigating conditions provide for the passage of time and actions of the subject to demonstrate that he/she is no longer involved with drugs. For personal use, experimental abuse is not as serious as regular or compulsive abuse because of the less serious effects on the subject. Possession of paraphernalia for personal use is not as serious as possession for manufacture.

The subject's involvement in sale, trafficking, distribution, cultivation, etc., is the most serious as he/she is now involved for profit. Accordingly, the mitigating information requires a longer period of time and other conditions. When involved in these latter acts, the subject is affecting other persons and the effects on them cause a larger problem.

People try drugs on an experimental basis just to see what they are like. They are curious or sometimes there is peer pressure. People attend rehabilitation programs for three primary reasons as shown in Figure 5-9.

Reasons for Rehabilitation Programs

- o A court orders the subject into a rehabilitation program as a result of some criminal or civil act.
- o The subject is "talked into" going into a program by relatives, friends, counselors, ministers or others trying to help him/her.
- o The subject recognizes that he/she has a problem and voluntarily seeks help.

Figure 5-9

The adjudicator is interested in how the person got into a program and whether he/she successfully completed it. **People who successfully complete a program are better risks than people who fail to complete or even attend one.**

Review Assignment

Review paragraph 2-200n (page II-3) and the adjudication guideline for Drug Involvement (NOV 98 MEMO) before reading the examples. The three examples show information that you will see about drug abuse and how the disqualifying and mitigating conditions are applied.

Example 1

The subject is a newly selected civilian employee on whom a SSBI is being conducted for a Top Secret clearance. During the interview portion of the SSBI, the subject states that she uses marijuana about once or twice a month or at parties if it is offered. **The subject states that she will not use marijuana at work but will continue to use it as before.** She does not see anything wrong with its use if it does not affect the job.

A statement of intent to continue using drugs cannot be mitigated.

In this example, the subject's **stated intent** to continue using marijuana, even away from the job, is sufficient to cause an unfavorable decision. The subject has shown that she will continue to violate laws and be influenced by marijuana. The subject's **trustworthiness and reliability** are in question; therefore, **the decision is unfavorable.**

Example 2

A military member has a Secret clearance. The activity receives a criminal investigation report that shows the subject sold cocaine to undercover agents on two occasions. The subject was apprehended, the activity suspended the access to classified information and reported it to the CAF.

In the subject's statement to the agents, **she said that she wanted more money than the military was paying her, so she sold drugs to make the money.** She had been selling drugs to other military personnel for about six months. The subject was charged with a violation of the Uniform Code of Military Justice and a date was set for the court-martial.

In this example, the sale of drugs over a period of time is disqualifying in itself. **Due to the recency, there are no mitigating conditions** to apply in this case; therefore, an unfavorable decision would be made. The example points out three of the adjudicative guidelines for criminal conduct, financial considerations and drug involvement. Drug involvement information will also involve criminal information as possession or sale are criminal acts.

Example 3

The individual is a newly selected **summer hire** employee for a noncritical-sensitive position requiring a Secret clearance.

The subject listed his drug use on the SF 86 for the NACLIC. The activity let the employee come to work but did not grant the interim security clearance pending a CAF final determination. DSS expanded the NACLIC to obtain a

subject interview and record checks for information about his drug use.

The statement in the Expanded NACLIC indicated that the subject used marijuana for about four years on a "frequent" basis. The last time he used marijuana was about two years ago. The subject's parents placed him in a rehabilitation program which he successfully completed.

The subject indicated that he would never use illegal drugs again. The record check of the clinic showed the subject did successfully complete the rehabilitation program.

The local agency checks turned up no arrest or detention information about the subject.

In this example, the subject used marijuana on a frequent basis for four years. **Mitigating this is the successful rehabilitation program, the fact that the subject has not used marijuana for over two years, the subject's statement of no future use, and no arrests or other criminal information.** The subject has shown a positive improvement in the last two years. Based on this information, **a favorable determination could be made.**

Summarizing the Examples

The three examples all contain disqualifying information. **The first example** cannot be mitigated due to the subject's statement about future use. **The second example** is too recent in time to make any adjudicative decision other than an unfavorable one. **The third example** contains sufficient mitigating information to make a favorable determination.

If there is drug abuse, there is criminal conduct.

The drug abuse examples illustrate how more than one adjudicative guideline can be included in evaluating information. The focus has been on individual guidelines even though others may have been present.

The different guidelines have not been interrelated to the point that we must consider disqualifying and mitigating conditions of several guidelines at once.

The example in the "Multiple Issues" section of this lesson will combine information based on several of the adjudication guidelines.

PERSONAL CONDUCT

This adjudicative guideline addresses conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations that could indicate that the person may not properly safeguard classified information. **This includes refusal to cooperate and falsification issues.**

First, we will discuss falsification issues.

Falsification is an attempt to conceal, misrepresent, omit or create false qualifications.

Falsification is used by a subject to deliberately conceal, misrepresent, omit information or create false qualifications when providing information to a Federal agency. The purpose of the falsification may be to conceal information from the agency which could prevent employment, granting of a clearance or some form of benefits or awards.

Or he/she may create false qualifications to get a job, security clearance, award or other benefit. In either case, the subject is intentionally not providing true and accurate information to the Federal agency. **This conduct calls into question the subject's trustworthiness and reliability.**

The subject may not provide information because he/she does not understand the questions, an oversight or because of improper instructions on how to complete the forms. In these cases, the subject is not intentionally falsifying the information. **The subject must be informed of the need for the information and given the opportunity to provide it.**

When you are reviewing a potential falsification issue, look at the relevance of the information. Is the information material to evaluating the subject's loyalty, trustworthiness

and reliability such as criminal activity, financial matters, fired from a job, etc. Or, is it immaterial to making the determination, such as an oversight of forgetting to list a seven-year old \$125 traffic fine.

When evaluating a personal conduct issue, ask yourself two questions. **Was the falsification deliberate or inadvertent? Is the information relevant or immaterial?** The answers make the difference between a favorable and unfavorable determination.

Deliberate Falsification

Falsification frequently involves hiding information relevant to a personnel security determination. Occasionally, it will involve the creation of qualifications needed to get a job when the subject does not actually possess them. You must use your **common sense** to determine if the falsification was deliberate, considering the available information.

Review Assignment

Review paragraph 2-200o (page II-3) and the adjudication guideline for Personal Conduct (NOV 98 MEMO) before reading the examples. The two examples show the types of information you will see and how the disqualifying and mitigating conditions are applied.

Example 1

The subject is completing the SF 86 as part of a SSBI package. The subject is supposed to list all convictions except those traffic violations which resulted in a fine of less than \$150 (unless it involves drugs). The subject forgets to list a traffic fine of \$200 for reckless driving seven years ago. The completed SSBI shows the reckless driving conviction.

Is this a serious enough falsification to make an adverse determination? If there is no other disqualifying

information or falsification in the case, then forgetting to list the one traffic conviction would not be serious enough to make an unfavorable determination. The omission of the conviction would appear to be something a person could reasonably forget due to the time period.

The mitigating conditions in the example would be:

The information was not material enough by itself for an adverse decision.
It was an isolated falsification.
The falsification was not willful.

Figure 5-10

***Use common sense.
Is it something that
is minor and easy to
forget?***

The instructions the subject received on completing the form may have given the impression that the traffic offenses were not what they were looking for. One of the problems in completing forms is that the instructions an official gives may not be correct. The subject may follow them in good faith even though the forms require the information. This example would result in a favorable determination.

Example 2

The activity is reviewing a completed ANACI on a new civilian employee selected for a noncritical-sensitive position. The employee is working in the position with an interim Secret clearance. When the interim clearance was granted, there was no derogatory information known. The completed ANACI contains a local agency check that shows the subject is currently on probation for felony theft. The activity security office suspends the access to classified information, but the activity personnel office makes a

favorable employment decision because the subject's criminal conduct would not affect the current job.

In this example, the omission of the criminal conduct and current probation is clearly a deliberate falsification. It is unlikely the subject could forget that he is currently on probation for a felony crime. **There are no mitigating conditions in this example; therefore, the decision would be unfavorable.**

PERSONAL CONDUCT, (CONTINUED)

A subject refuses to answer in order to hide something or believes it is no one else's concern.

This portion of the adjudicative guideline, Personal Conduct, involves the **refusal to provide information, or refusal to cooperate** with required security processing, investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination. A subject refuses to provide information because either he/she does not want the information known or believes it is not anyone else's business to know the information. Unless the disclosure of the information is precluded by law or regulation, the subject is required to provide to the government any relevant information needed to determine his/her trustworthiness, reliability or judgment.

Considering a Subject's Refusal to Cooperate

When considering a subject's refusal to provide information, or access to it, the subject must be informed of the potential consequences of the refusal. The following actions will be taken by the activity if the subject refuses to provide information or releases, or to authorize other persons to provide the information:

- **Suspend processing of the request for investigation and personnel security determination.**

- **If the subject has access or performs sensitive duties, suspend access to classified information until the information is provided,.**
- **Notify the CAF.**

Upon notification that the subject has refused to provide the information, the CAF must notify the subject of the potential consequences of his/her actions. The subject would not be eligible to have access to classified information or assignment to sensitive duties until the information is provided and evaluated. If the subject refuses to comply, the CAF would start an adverse personnel security determination per paragraph 8-201 of the regulation (See Lesson 4, Due Process.)

This action is taken because there is, or is believed to be, information available that must be considered in a personnel security determination. The subject has intentionally not provided the information or access to it; therefore, the adjudication would not be based on complete information. Since there was missing information, the determination could not be clearly consistent with the interests of national security as there is an unanswered question about the information.

A CAF may notify the subject by one of two means:

- **Upon notification by the activity that the subject has refused to provide the information, notify the subject in writing about the requirement and the consequences.**

If the subject provides the information, the processing will continue. If not, the CAF issues a Statement of Reasons (SOR) proposing the denial of security clearance or assignment to sensitive duties for the failure to provide information or

- **Upon notification by the activity that the subject has refused to provide the information, the CAF may send an SOR stating that the**

reason for the action is the subject's failure to provide the information.

The SOR would inform the subject of the requirement and consequences of the failure. If the subject provides the information, the SOR can be withdrawn and processing continues. If not, the CAF would make a final adverse determination.

Review Assignment

In 2R review paragraph 2-200p (page II-3) and the adjudication guideline for Personal Conduct (NOV 98 MEMO) before reading the examples. The two examples show the types of information you will see about refusing to provide information and how the disqualifying and mitigating conditions are applied.

Example 1

The subject refuses to provide a release authorization to obtain records about his hospitalization for a mental disorder. The activity informs the subject that the information is needed for a determination of his eligibility to be granted a security clearance. If it is not provided, processing of the investigation request will stop. He will not be eligible to have access to classified information or be able to perform sensitive duties until the information is provided and evaluated. Upon being notified of the requirement, the subject signs the release and the investigative process continues. The adjudication will be made based on evaluation of the PSI results, including the medical information.

Example 2

We will use the same circumstances as the first example except after being advised of the requirement and consequences, the subject still refuses to provide the release. The activity then suspends processing and notifies the CAF. The subject will not be permitted to have access to classified information or perform sensitive duties until

the information is provided. The CAF then formally notifies the subject of the requirement and consequences with an SOR. If the subject still refuses to provide the release, the CAF will make an unfavorable personnel security determination. The adverse decision will remain in effect until the information is made available and adjudicated. Then the decision will be based on evaluation of information, not a refusal to provide information.

Remember!

A key point to remember when a subject refuses to provide information/releases, or authorize others to release information, is that the subject must be aware of the requirement and the consequences of the refusal. If not, then a final action cannot be taken by the CAF until he/she is notified. In the majority of cases, the subject will provide the information when informed.

SEXUAL BEHAVIOR

Personal bias check!

This adjudicative guideline involves acts of sexual behavior or perversion which may indicate a personality or emotional disorder, poor judgment or criminal conduct. Information about sexual behavior is generally developed through police and medical information. Sexual orientation or preference may not be used as a basis for, or a disqualifying condition in, determining a person's eligibility for a security clearance.

Review Assignment

Review paragraph 2-200q (page II-3) and the adjudication guideline for Sexual Behavior (NOV 98 MEMO) before reading the examples. Three examples show the types of

information you will see involving sexual behavior and how the disqualifying and mitigating conditions are applied.

Example 1

The subject has been selected for a Non-Appropriated Fund position of trust as a day-care worker. The subject's SF 85P NACLIC did not contain any derogatory information; therefore, the subject was permitted to go to work in the military day-care center. The completed NACLIC contains an arrest record indicating the subject was convicted on three charges involving minor children. Nine years ago, the subject was convicted of child molestation (felony) and three years ago he was convicted of Lewd and Lascivious Acts and Contributing to the Delinquency of a Minor (both misdemeanors). DSS was requested to conduct an SII to obtain further information about the criminal acts and possible medical information. A subject interview disclosed he received counseling ordered by the court after the molestation conviction. The court records showed the subject had been the victim of child abuse and this was a contributing condition in the subject's conduct. The subject successfully completed the rehabilitation program with a medical opinion that he realized the problem and could now cope with it. There was little likelihood of any similar misconduct in the future. The two recent convictions involved sexual acts with minor children while working at a day-care center. There were no other counseling or therapy records available.

The CAF referred the SII to the activity for an employment determination. The activity removed the subject from the position as unsuitable to care for minor children.

If the case had required a personnel security determination, then several adjudicative issues were present:

- The subject had falsified the SF 85P by not listing the criminal or mental treatment information.
- There have been three instances of sexual behavior within the last nine years.

- The subject successfully completed a rehabilitation program with a favorable medical prognosis but subsequently committed two further acts of sexual behavior.
- There is no current medical information about the subject's condition.

In this example, there is a question about the subject's trustworthiness and reliability due to the incidents of sexual behavior. The original medical opinion is not supported by the recent events and the current medical status is unknown. If a personnel security determination had been requested, a current medical evaluation would not be beneficial because of the recent acts of sexual behavior. A period of time would be necessary before a review would be appropriate. The information in the example is sufficient to warrant an adverse determination.

Example 2

The subject has been selected for a critical-sensitive position to perform fiduciary duties as the deputy procurement officer. The subject's SF 86 for the SSBI shows he has been arrested three times for wife and child abuse. It also shows that he has received professional counseling for his problems. The activity requests the SSBI, but does not ask for an advance NAC for an emergency appointment. The subject is told not to report for work until the SSBI has been completed and adjudicated.

The completed SSBI is being reviewed at the CAF. The interview reveals the subject had gone through some difficult times about ten years ago due to his brother slowly dying from cancer and leukemia. The subject was upset because he would go to the hospital and become extremely frustrated that the doctors could not do more for his brother. He took out his frustrations on his wife and child in a one-month period by sexually assaulting his wife on one occasion and beating his wife and child on two other occasions. He was arrested each time but his wife would

not testify in court; therefore, the subject was not convicted of any crimes. The subject agreed to seek professional counseling because of the effects on the family. The brother died shortly after the subject entered counseling. The counseling helped the subject to recognize the problems and deal with the frustrations. The psychiatrist stated the reactions were situational due to the condition of his brother, but there should be no permanent effects or future problems with the subject. The subject should lead a normal life according to the doctor.

There have been no further incidents since the counseling about ten years ago. The subject states that he is able to recognize the problems and could deal with them in the future without harming himself and the family members. A favorable decision is made by the CAF and the subject is employed in the position.

In this example, there was sexual behavior, wife and child abuse ten years ago. The reason for the behavior was due to a temporary situation, but counseling helped the subject to recognize and deal with the problem. The medical opinion indicated that there should not be any future problems and there have been no incidents since that time. **There is sufficient mitigating information to make a favorable determination.**

Example 3

The subject occupies a noncritical-sensitive position with a Secret clearance. A local police report is received that shows the subject was recently arrested for two counts of rape. The access to classified information is temporarily suspended and the report is sent to the CAF. DSS is requested to conduct an SII to obtain details and disposition of the charges. The completed SII is being reviewed at the CAF. The subject had made a confession to the local police indicating he had liked the two women, spent time and money on them, and then forced them to have sexual relations with him. The subject stated a belief that if he spends time and money on a woman, he is entitled to have sex with her. The charges against the subject were dismissed because the police had not properly

advised the subject of his rights before he made the confession.

In this example, there is a statement by the subject that he did forcibly have sexual relations with the two women. He was not prosecuted due to a legal technicality. His statement raises questions about his future conduct as he believes he is entitled to have sex with a woman if he spends time and money on her. The conduct was intentional, criminal, forcible and there is a question about future behavior. There is no information to mitigate this right now. **The disqualifying information is sufficient to make an unfavorable determination.**

Summary of the Examples

Subjects are unwilling to Discuss their sexual activities.

The three examples show that sexual behavior information is generally surfaced by police or medical information. Subjects are often unwilling to disclose this type of information as it is both personal and embarrassing. This also makes the subject vulnerable to blackmail, pressure or coercion. Once the information is known, it will reduce the vulnerability, but not eliminate it. You should be aware that counseling is not always required by courts after the behavior. In many cases there will be private counseling, but no information about it is developed in the PSI. **The SII is a means to develop that type of information.**

OUTSIDE ACTIVITIES

This guideline pertains to certain types of outside employment or activities that DoD personnel may get involved with, that may be of a security concern, and how these types of activities and employment will be evaluated. The concern arises when an individual's employment or activity poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized DSS closure of classified information.

Foreign connections of any kind (relatives, friends, business interests, etc.) are to be thoroughly investigated as potential security issues. When the PSQ lists or the investigation develops these connections, efforts will be made to obtain as much information as possible through interviews or records checks.

Many times an individual will engage in outside employment or activity without realizing that it may pose a risk to the national security. An individual may be moonlighting with a company that sells products and commodities to foreign interests or may even be owned by foreign nationals.

Individuals in this type of situation must be made aware of the possible conflicts of interest, and attempts to obtain technical or scientific information from him or her, and similar considerations, because of their security responsibilities.

Individuals engaged in outside employment should evaluate the company or activity because of the potential risk involved. The individual may opt to DSS continue the employment or the activities after taking a closer look at the company or activity.

Special agents or security managers will advise the Subject regarding proper actions to be taken if he/she is ever approached to provide information to unauthorized personnel.

Evaluating Outside Activity Information

When evaluating information about outside activities, you must consider **any** service or employment (whether compensated or not) with: **any** foreign country; **any** foreign national; or **any** representative of a foreign interest.

Individuals who are associated with a foreign country, foreign national, or foreign representative, as mentioned above, would be more easily targeted by foreign intelligence than one who has no such contact.

Individuals with **any** type of association mentioned above must report this type of service to their security managers.

Any service or employment (whether compensated or not) with:

Any organization or person engaged in analysis, discussion, or publication of materials about intelligence, defense, foreign affairs, or protected technology.

In some cases, there may be a FOCI (Foreign Ownership, Control, or Influence) issue. A military member or civilian employee cannot, at the same time, be a representative of a foreign interest. By law, that is a conflict of interest because the individual would be looking out for the interests of a foreign country or corporation while their allegiance is to the U.S. for military or civilian service. For contractors, this is handled on a case-by-case basis.

When mitigating conditions are present, a favorable decision is possible . Mitigating conditions include:

- The employment or activity does not pose a conflict with the individual's security responsibilities.
- The individual terminates the employment or activities when notified that there is a potential conflict with the security responsibilities. After the individual terminates the employment or activity, there must be no further involvement with the former employer or activity.

Many questions will need to be addressed when the PSQ lists, or the investigation develops these issues, regarding outside activities.

These questions include the full identity of the activity or foreign connection; the degree, extent, and purpose of such activity or connection; any relationship of subject to persons associated with the activity or foreign connection; whether the activity or connection may make the subject and his/her immediate family vulnerable to coercion, influence, or pressure.

These are only a few of the questions that must be answered when outside activities indicate a potential for a conflict of interest due to issues mentioned in this adjudicative guideline.

Review Assignment

Review the adjudication guideline for Outside Activities (NOV 98 MEMO).

MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

This guideline involves automated systems that the Department of Defense (DoD) relies on to accomplish the primary missions and support functions.

The misuse of information technology systems (ITS) is of security concern as it degrades the mission capability and confidence in the systems.

ITS are used for a variety of functions, both primary and support.

Primary Uses of ITS

- **Classified ADP.** This involves the use of secure systems to process classified information at all levels. ITS are used to process Sensitive Compartmented Information (SCI) and Special Access Programs (SAP) information.
- **Sensitive ADP.** This involves information that is protected, but not classified. Examples are: Privacy Act information; bid information; proprietary information; medical information; and high dollar value items.

- **Weapons systems.** Many of our “high tech” weapons systems and platforms are dependent upon ITS to operate. Examples are: aircraft; ships; submarines; missiles; artillery systems; and tanks.
- Also, other platforms depend on ITS for their operation. Examples are satellites and communication systems.

ITS is used in many of our support systems, such as supply operations. The concern here is the dollar value of equipment and materials that have to be replaced.

Misuse of ITS can have varying effects, from serious national security issues to dollar value losses.

Examples are:

- Classified information contained in ITS can be compromised.
- Unclassified, sensitive information may be copied from the ITS. This can result in the loss of protected information. Examples are: Privacy Act information; proprietary data; bid information; and other protected information.

It may be used for unauthorized purposes. An example is selling mailing lists of employees/military members to commercial firms.

- There can be a dollar value loss. If material is diverted and used for personal gain or other unauthorized uses, it must be replaced to meet its initial purpose. **Examples are:** computers; parts; and general supply items.
- Misuse can result in the compromise of a secure system or even its loss. Additional time and money is necessary to fix and re-test or re-certify the system.

- The system can be damaged by misuse. Additional time and money is necessary to fix and re-test or re-certify.
- Misuse can result in denial of access to the system. This would delay mission accomplishment and be costly to fix and re-test or re-certify.
- All of the above situations result in degraded mission capability.

An example of degrading mission capability occurred in 1995 at a DoD medical laboratory.

The mission of the laboratory was to evaluate drug testing samples. Two civilian employees falsified the results in the computer system by taking positive results and showing them as negative. Their intent was not to help people get around the drug screening, but to reduce their own workload. Positive results required additional work and they did not want to do the extra work. This practice was discovered when another employee noticed the quality control samples that were supposed to be positive were shown as negative in the system.

This resulted in questions being raised about the accuracy of the drug testing. Laboratory personnel had to go back over the results and re-test the samples to ensure they were accurate. This misuse of an ITS resulted in a loss of confidence in the system, additional work and money to correct the problems to bring the system back to where it should be.

Misuse or noncompliance with the rules and procedures pertaining to ITS may raise a security concern about the individual's trustworthiness, willingness, and ability to properly protect those systems.

Potentially disqualifying conditions include:

Illegal or unauthorized entry into any ITS. This is someone who gets into the system illegally, such as a hacker. It also involves people who get into the system without authorization, such as someone using another person's password, or getting into the system when an authorized user leaves the terminal temporarily without using the security procedures to protect the data.

- o Illegal or unauthorized modification, destruction, manipulation, or denial of access to information in an ITS.

In these situations:

- o **Data may be compromised.**
- o **Data may not be available or used for unauthorized purposes.**
- o **The system may be damaged or the use prevented or delayed.**

Other potentially disqualifying conditions are:

- o Removal or use of hardware, software, or media from any ITS without authorization or when prohibited by rules, procedures, guidelines, or regulations.
- o Introduction of hardware, software, or other media into any ITS without authorization or when prohibited by rules, procedures, guidelines, or regulations.

In these situations, the integrity of the ITS may be compromised or its intended use may be prevented. In the case removal, the individual may be converting it to personal or other unauthorized use.

Mitigating conditions include:

- The misuse was not recent or significant.
- The conduct was unintentional or inadvertent.
- The introduction or removal of media was authorized.
- The misuse was an isolated event.
- The misuse was followed immediately by a prompt, good faith effort to correct the situation.

MULTIPLE ISSUES

Multiple issues involve the inter-relationship of two or more guidelines.

Many of the cases you will see contain multiple issues. These are cases where the information involves more than one of the adjudicative guidelines. Some cases may involve several of them. There may be disqualifying information from each of the guidelines but there may not be mitigating information from each one. Several of the examples shown in the above guidelines contained multiple issues. This is because of interrelationship of the types of conduct and conditions. Multiple issue cases are decided by more senior adjudicators due to the complexity of the cases.

An Example

One example of a multiple issue case will be given to show some of the considerations in making a personnel security determination. In this example, the subject has been selected for a critical-sensitive position requiring a Top Secret clearance. The SSBI request package and local files check disclose no derogatory information. The activity requests an advance NAC so they can consider an emergency appointment and interim Top Secret clearance.

The NAC reveals quite a list of arrests without dispositions, so DSS starts expanding that information while the SSBI is running. The completed SSBI is sent to the CAF.

The information includes:

- Criminal Conduct
- Alcohol Consumption
- Drug Involvement
- Emotional, Mental and Personality Disorders
- Financial Considerations
- Personal Conduct
- Sexual Behavior

The PSI includes:

- Police reports
- Hospital and clinical reports
- Credit reports
- Court records
- Reports from previous employers
- Psychiatric evaluations
- Drug and alcohol counseling records
- Neighborhood information
- Confidential informants
- State unemployment reports

To sum up the information, the subject has a history of:

- Thirty-five arrests for rape, aggravated assault, robbery, bad checks, drug sales, drunk in public, unemployment fraud, etc., over the past fifteen years with twenty-one convictions.
- The subject has been diagnosed as a paranoid schizophrenic with periods of violent relapses. The subject mixes alcohol, cocaine and PCP with his nerve medicine to get a “high”.
- The subject collected state unemployment insurance when he was actually working.
- The subject wrote 31 bad checks. The subject failed to complete a court ordered mental health counseling program after an assault conviction.
- The subject would not discuss the treatment for mental illness with the DSS agent, only provided some releases, and there were other hospitalizations that DSS could not get releases for.
- The subject did not reveal any of this information on the SF 86.

Whew!

The information in this example was taken from an actual case received by a CAF for adjudication. There had been a favorable employment determination as the activity decided none of the information had a direct bearing on his job. Most multiple issue cases are not quite this involved, but some are. This is just an example of the type of cases adjudicators see and review for a final determination. By the way, the subject did not get the clearance.

SUMMARY

This lesson explained what types of information, disqualifying and mitigating, make up suitability issues. Examples were provided to show the types of information you will see and how it is evaluated. The lesson also explained the interrelationships of the guidelines and how cases may contain multiple issues. We did not go into detail on resolving all issues in the multiple issue case because senior adjudicators make determinations on those cases. We will talk about that in the resident phase of the Adjudicator's Course and in the Advanced Adjudicator's Resident Course.

Review Exercises

1. The security criteria of paragraph 2-200a-q are used to determine eligibility for clearance.
 - a. True
 - b. False

2. Which of the following PSIs would be used to obtain information on derogatory information received after the initial PSI had been conducted and adjudicated?
 - a. Personal Interview
 - b. SII
 - c. PR
 - d. SSBI

3. An individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior.
 - a. True
 - b. False

4. Information that a subject with a security clearance is involved in current criminal activity should be referred to DSS for an investigation.
 - a. True
 - b. False

5. What are the two major categories of adjudication issues?
_____ and _____

6. What are the nine conditions used in evaluating information?

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____
- f. _____
- g. _____
- h. _____
- i. _____

7. A pattern of negligent conduct in handling or storing classified documents may be a disqualifying condition of which adjudication guideline?

- a. Allegiance to the United States
- b. Foreign Preference
- c. Security Violations
- d. Foreign Influence

8. Lack of knowledge of the unlawful aims of an organization may be a mitigating condition of which adjudication guideline?

- a. Allegiance to the United States
- b. Foreign Preference
- c. Security Violations
- d. Foreign Influence

9. Allegiance issues are the most significant and potentially damaging issues to National Security an adjudicator will review.

- a. True
- b. False

10. What are the three adjudication guidelines most often associated with allegiance?

- a. _____
- b. _____
- c. _____

11. Suitability issues involve any behavior, condition, circumstance or other condition that directly affect the subject's trustworthiness or reliability.

- a. True
- b. False

12. A PSI will contain only one type of suitability issue.

- a. True
- b. False

13. What are the thirteen adjudication guidelines used to evaluate suitability information?

- a. _____
- b. _____
- c. _____
- d. _____

- e. _____
- f. _____
- g. _____
- h. _____
- i. _____
- j. _____
- k. _____
- l. _____
- m. _____

14. Review the following example. Identify the adjudication guideline(s) you would use to evaluate the information for a personnel security determination.

The subject is a native-born United States citizen who is a civilian employee and occupies a noncritical-sensitive position. He currently has a Secret security clearance. The subject secretly belongs to a group that believes in the unlawful overthrow of the current United States government. The group plans to violently disrupt the operations of a military base to draw attention to their cause. The subject uses his access to classified information to obtain a copy of the classified emergency plan of a military base. He gives the plan to the group leader. The plan will be used to identify targets on the base and security force response action/times. This will help the group's members to plan their operations and an escape route after the attack. End of example.

ANSWER:

15. Review the following example. Identify the adjudication guideline(s) you would use to evaluate the information for a personnel security determination.

The subject is a civilian employee in a critical-sensitive position with a Top Secret security clearance. The activity receives a report from the local police department indicating the subject was arrested for theft (felony) on January 5, 1988. On March 7, 1988, the subject pled guilty to a reduced charge of petty theft (misdemeanor), was fined \$250, and given a one-year suspended sentence. A CAF adjudication was requested. End of example.

ANSWER:

Solutions & References

1. a. True (DoD 5200.2R, para 2-200)
2. b. SII (DoD 5200.2R, para 2-306)
3. a. True (DoD 5200.2R, Appendix I, Lesson 5 page 12)
4. b. False (DoD 5200.2R, para 2-402d)
5. Allegiance and Suitability (Lesson 5, page 5-3)
6. (Lesson 5, page 5-10)
 - a. Nature, extent and seriousness of the conduct
 - b. Circumstances surrounding the conduct
 - c. Frequency and recency of the conduct
 - d. Age of the subject at the time of the conduct
 - e. Voluntariness of the participation
 - f. Presence or absence of rehabilitation
 - g. Motivation of the conduct
 - h. Potential for pressure, coercion, exploitation or duress
 - i. Likelihood of continuation or recurrence
7. c. Security Violations (NOV 98 MEMO)
8. a. Allegiance to the United States (NOV 98 MEMO)
9. a. True (Lesson 5, page 5-13)
10. (Lesson 5, page 5-14)
 - a. Allegiance to the United States
 - b. Foreign Preference
 - c. Security Violations
11. a. True (Lesson 5, page 5-20)

12. **b. False (Lesson 5, page 5-69)**
13. **(Lesson 5, page 5-3)**
 - a. **Security Violations**
 - b. **Criminal Conduct**
 - c. **Emotional, Mental and Personality Disorders**
 - d. **Misuse of Information Technology Systems**
 - e. **Financial Considerations**
 - f. **Alcohol Consumption**
 - g. **Drug Involvement**
 - h. **Personal Conduct**
 - i. **Outside Activities**
 - j. **Sexual Behavior**
 - k. **Allegiance to the U. S.**
 - l. **Foreign Influence**
 - m. **Foreign Preference**
14. **Allegiance, Security Violations and Criminal Conduct (NOV 98 MEMO)**
15. **Criminal Conduct (NOV 98 MEMO)**

LESSON 6

CONTINUOUS EVALUATION

In this lesson you will learn why the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action.

We will discuss why the individual's trustworthiness is a matter of **continuing assessment**, and what responsibilities management, supervisors and individuals have for continued security eligibility.

We will also discuss the briefings that management must give the employee to insure they know their responsibilities and how to meet them.

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

- ◆ What responsibilities does management have for continuous evaluation?
- ◆ What responsibilities do supervisors have for continuous evaluation?
- ◆ What are the individual's responsibilities for continuous evaluation?
- ◆ What are the co-worker's responsibilities for continuous evaluation?

READING ASSIGNMENT

Attachment 1:

DoD 5200.2R Chapter 9: Sections 1

Continuous Evaluation

Uninterrupted assessment of a person for retention of a security clearance or continuing assignment to sensitive duties



The first security clearance

Figure 6-1

The continuous evaluation process prescribed by Chapter 9, DoD 5200.2-R, requires that persons who are authorized access to classified information or perform sensitive duties continually meet certain standards of trustworthiness, reliability, and loyalty. The disqualifying and mitigating criteria and conditions in Chapter II and Nov 98 memo reflect the standards in detail.

However, except for selected positions or when resolving derogatory information, we conduct a PSI only in support of the initial determination. Even when the nature of the position calls for recurring investigations, the reinvestigations are at least five years apart.

Adverse changes occur.

If we rely solely on these investigations for continued access, we are not recognizing that adverse changes occur in some employees' lives which create substantial doubt as to their qualifications. We need to know what is happening in their lives on a current basis to insure that they are still trustworthy.

The continuous evaluation process is necessary to evaluate the individual's post-adjudication activities by the same standards of trustworthiness, reliability, and loyalty used in the actual adjudication. DoD 5200.2-R imposes responsibilities on DoD components, commanders, supervisors, individuals, and co-workers to meet continuous evaluation requirements.

RESPONSIBILITIES

At component level.

The Heads of DoD Components establish and maintain a program to evaluate, on a continuing basis, the status of personnel under their jurisdiction with respect to security eligibility.

The programs try to insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process. Heads of components are encouraged to establish counseling and assistance programs to identify and correct problems early.

Need briefings.

Commanders and heads of organizations insure that personnel assigned to sensitive duties are initially indoctrinated and periodically instructed thereafter on the national security implications of their duties and their individual responsibilities.

PROGRAMS

Supervisors review PSQs.

Supervisory personnel learn their special responsibilities pertaining to personnel security for persons they supervise, what to report, what actions to protect national security interests are necessary, and the help available to aid individuals in overcoming problems. Additionally, they review PSQs on subordinates when prepared as part of a PR request and, based on information they know, include a statement on whether they know of disqualifying criteria.

Appraising security performance.

Further, in regularly scheduled fitness and performance reports on military and civilian personnel who have access to classified information, their supervisors appraise their performance of security responsibilities.

Continuous Evaluation.

The commander or director of an organization establishes procedures to insure that information which could reflect on each individual's trustworthiness are promptly identified and evaluated. **Within the organization, the commander sets up a program of continuous evaluation.** This program taps those sources of information and treats the information with the confidentiality necessary to protect the security of the United States and protect the rights of the individual. The information is acted upon in the most effective manner to ensure that rapid and appropriate resolution is made of the matter.

ACQUIRING INFORMATION

Sources of pertinent information.

The essential element of a continuous evaluation program is acquiring pertinent information concerning the suitability, loyalty, and trustworthiness of individuals without violating their rights. The following principles and concepts apply to what could otherwise be considered an intrusive and unwarranted invasion into the privacy of the individuals:

- Obligation to Report.*** ◆ DoD personnel have an obligation to report information that reflects an **actual or potential** danger to national security.

- Coordination & Education.*** ◆ Effective coordination with and education of potential sources of information is needed to insure that they are identified and reported in a manner which protects the interests of the government and the individual.

- Respect for Privacy.*** ◆ Respect for privacy and confidentiality of information received is essential.

- Prompt resolution.*** ◆ Prompt action to resolve unfavorable information is necessary both to protect the individuals involved and the activity.

- People change.*** ◆ People and their situations change over time for better or for worse.

- Continuous Support.*** ◆ Support from the activity's command, staff, and personnel must be continuous and consistent.

SOURCES OF INFORMATION

There are many sources of information available for continuous evaluation. Among the most important are the ones within the command itself. They are:

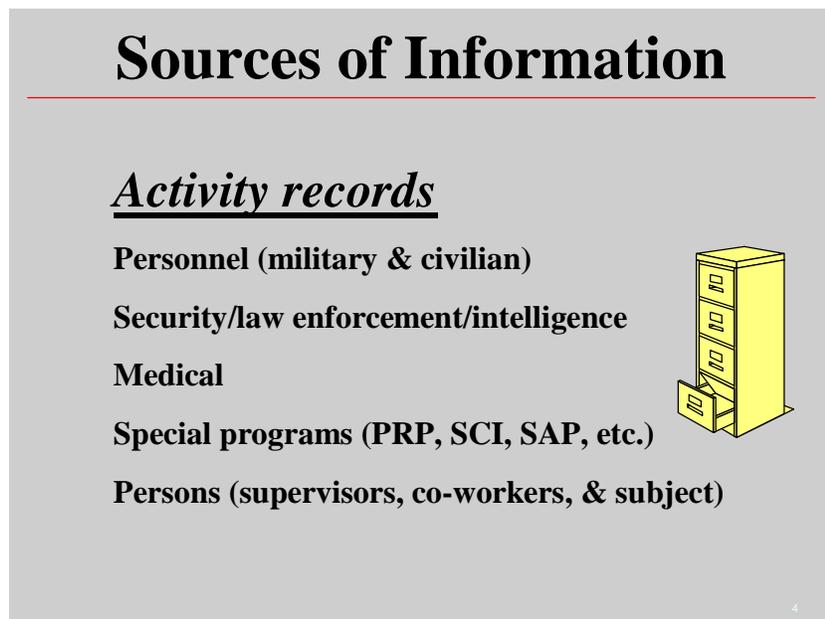


Figure 6-2

- ✓ **Command/Activity.** The commander/director is involved in a variety of disciplinary and corrective personnel actions which involve matters such as Article 15 punishments, letters of indebtedness, performance and conduct counseling, and other supervisory problems.
- ✓ **Personnel files.** Military and civilian personnel offices are involved not only in the investigation of suitability for employment but also handle the Suspensions of Favorable Personnel Action, so called "flagging actions" on military personnel who have unresolved unfavorable information.

- ✓ **Security/Law Enforcement/Intelligence files.** These files contain past and present allegations.
- ✓ **Medical files.** Several types of DoD medical facilities are a local source of information concerning physical or mental illnesses which could disqualify a person for sensitive duties.
- ✓ **Special program files.** (Personnel Reliability Programs, Sensitive Compartmented Information, Human Reliability, etc.) The files maintained by special program managers contain information which is used for essentially the same purposes that our continuous evaluation program are.

Reporting Information

Supervisors & Co-Workers



- Anything that affects duties
- First to know of information
- Report for safety reasons

8

Figure 6-3

Supervisors and co-workers. Persons working in the general proximity of an individual can become aware of disqualifying factors through their close association. They should be the first to note if an individual has problems of a security concern or that may jeopardize their safety. Under the provisions of 5200.2R, they have an obligation to report that information promptly.

The chief of the activity, or designee, reviews such information and verifies it to assure it is pertinent and sufficiently serious to prompt action. That action may include suspending access, requesting an SII and notifying the CAF.

Reporting Information

The Individual

- Required to report information
- Unreliable in doing so
- To supervisor (work status)
- To Security Office



Figure 6-4

The Individual. A basic principle of personnel security investigation and of continuous evaluation is that the individual is the most knowledgeable source of personal information. The individual has the facts and can answer questions raised by the information. Individuals having access to classified information or performing sensitive duties are required by 5200.2R to notify their supervisors when their personal actions or circumstances violate the adjudication guidelines.

As you can well imagine, they are unreliable in doing so, and few of the individuals actually do report themselves. (Note: A few do report the conduct/behavior/violation as required. Some of those that do so also seek help through the Employee Assistance program (EAP).

- ✓ **Legal Assistance Office.** Legal assistance officials receive security related information such as indebtedness, civil suits, criminal actions, and domestic problems. After meeting ethical and legal standards of confidentiality, such officials have a responsibility to report derogatory information to security or commanders for review. Even if the content of the legal assistance/client relationship has confidentiality, the problem itself may be a matter of record.

- ✓ **Alcohol and Drug Abuse Programs.** While the content of alcohol and drug treatment programs and the counselor/client relationships are covered by confidentiality rules, the fact of attendance is normally a matter of record.

Sources of Information

Government Agencies



- Other Federal agencies**
- State governments**
- Local governments**

6

Figure 6-5

At the local activity the most frequent source of derogatory information from outside the command is **other federal agencies, state and local law enforcement agencies or governments.** The supporting military police or base security office is the normal recipient of such information.

SECURITY BRIEFINGS

Must know responsibilities.

The ability of an individual to continuously meet security responsibilities depends first on knowing what those responsibilities are and knowing how to meet them. Security education provides that knowledge and, in part, supports the continuous evaluation process. Accordingly, Components provide periodic briefings on security responsibilities to persons requiring access to classified information, or assigned to sensitive duties.

Training measures are grouped into the four security briefings (Figure 6-6) required by the personnel security program:

- ◆ **Initial Briefing**
- ◆ **Refresher Briefing**
- ◆ **Foreign Travel Briefing**
- ◆ **Termination Briefing**

Figure 6-6

In your adjudications, you should expect that the subject received these briefings and knew his/her responsibilities.

But the quality and methods of briefing will vary from activity to activity. If the content of the briefing is a critical factor in a case, this means you will probably have to request additional information.

INITIAL BRIEFING

The **Initial Briefing** is given after a determination of trustworthiness is made on an individual and before access is permitted. Once the person can be

How to protect.

trusted with the material, he/she must know how to **protect** the material. The initial briefing concentrates on the specific requirements for protection of the material to which the incumbent will have access and:

- ◆ **The techniques employed by foreign intelligence activities to obtain information and their responsibilities to report such attempts.**
- ◆ **The penalties for security violations.**
- ◆ **The requirement to report all foreign travel.**

Figure 6-7

The initial security briefing can be given by supervisory or security personnel but the activity is responsible to insure that no individual has access without the briefing.

REFRESHER BRIEFING

The **Refresher Briefing** is presented at least once a year for personnel having continued access to classified information. As a minimum, it covers the same topics required in the initial briefing.

FOREIGN TRAVEL AND CONTACT BRIEFINGS

The **Foreign Travel Briefing** applies to cleared personnel who plan travel in or through, foreign countries. The briefing is given prior to the travel. It alerts the traveler to possible exploitation by hostile intelligence services. They are **Brief and debrief** upon return as to what occurred during the travel.

This briefing is also required when such individuals will attend international, scientific, technical, engineering, or other professional meetings in the United States, or in any country where representatives of designated countries may be present.

When foreign travel patterns or failure to report such travel create a security concern, the activity refers the matter to their counterintelligence agency and the CAF. Records of briefings are maintained for five years.

TERMINATION BRIEFING

The **Termination Briefing** is given when an individual's employment is terminated, the security clearance is administratively withdrawn, or absence from duty or employment for 60 days or more is contemplated. The individual returns all classified material and executes a Security Termination Statement.

The Termination Briefing is also given to individuals who inadvertently gain access to classified information.

The Termination Briefing concentrates on continued protection for the information and includes the information shown in figure 6-8:

Termination Briefing

- ◆ **An acknowledgment that the individual has read and understands the implications of the laws and regulations for safeguarding classified information.**
- ◆ **A declaration that they have returned all classified material they possessed.**
- ◆ **An acknowledgment that the individual will report, without delay, to the FBI or the DoD component concerned any attempt by an**

unauthorized person to solicit classified information.

Figure 6-8

An individual's refusal to execute a Security Termination Statement is reported through the organization to DSS. DSS records that fact in the DCII.

THINGS TO REMEMBER

The granting of a favorable personnel action is not a final personnel security action. For as long as the individual is in a sensitive position, he/she remains the subject of continuous evaluation and education.

The continuous evaluation process is the day-to-day means we have of assuring our initial favorable security determination remains valid. It requires the involvement of the activity's management, supervisors, legal personnel, medical supporting agencies, the individual and their coworkers.

REPORTING AGENCIES

At this time, we will discuss CEP information coming to the CAF from sources other than the employing activity. You will learn which agencies are most likely to send this information to the CAF. We will also discuss the types of information each agency forwards to the CAF.

ADDITIONAL SOURCES OF INFORMATION

AT CAF LEVEL

As you learned in the last lesson, the employing activity is the source of most information sent to the CAF under the Continuous Evaluation Program (CEP). It is not, however, the only source of such information.

Information may be sent in by DoD agencies, other Federal agencies, state and local government agencies and by private individuals. Regardless of the source, any information received must be reviewed and adjudicated to determine its effects on the subject's current eligibility to perform sensitive duties or have access to classified information. You adjudicate this information in the same way as PSIs: review for completeness, relevancy, presence and resolution of issues and any disqualifying and mitigating factors, and obtain any additional information required.

The FBI

The Federal Bureau of Investigation is the major source of information sent to the CAF under this portion of the CEP. The types of information reported by the FBI reflect its dual mission: domestic counterintelligence (CI) investigations and criminal investigations involving violations of Federal laws.

In addition, the FBI maintains the National Crime Information Center (NCIC), which is a computer listing of arrests and convictions for violations of Federal, state and local laws as reported by law enforcement agencies. (NCIC is the computer checked in the "tech check" portion of the NAC.) NCIC reports (the FBI rap sheets or 1-4e Forms) are the largest share of information provided to the CAF.

The FBI is the major source of information.

Rap sheets are the most common FBI

Remember, though, that not all arrests are reported. Local practice and regulation determines what arrest information is reported to the NCIC. Even when arrests are reported, dispositions (convictions, acquittals, etc.)

information.

frequently are not. This means that you will frequently use the rap sheet as the basis for an SII request to DSS.

The FBI may also send CI and criminal investigations.

When the FBI has conducted a CI or criminal investigation which involves DoD affiliated personnel, you may receive a copy. This happens most often when the FBI is investigating an organization which the Department of Justice has determined to be subversive. If DoD personnel are involved with the group, the FBI may notify the appropriate CAF (depending upon whether such notification could compromise the investigation). Similarly, if the FBI is conducting an investigation into violations of Federal law, such as racketeering, the CAF may be notified about any DoD personnel involved.

The various reports sent in by the FBI are unsolicited; that is, they come to the CAF without being specifically requested. Most Components have standing reporting agreements with the FBI for the CAFs to receive all available information.

DoD Criminal Investigative Agencies

CID, NCIS, and AFOSI conduct criminal investigations.

Each of the military departments (the Army, Navy and Air Force) has its own criminal investigating agency. Army has the Criminal Investigations Command (CID), Navy has the Naval Criminal Investigative Service (NCIS), and the Air Force has the Office of Special Investigations (AFOSI). In addition, the Defense Criminal Investigative Service (DCIS) provides certain investigative assistance (primarily in the area of waste, fraud and abuse) to DoD agencies.

The Component criminal investigative agencies provide investigations relating to crimes against the Component or crimes committed on government property. You will frequently see CID, NCIS and AFOSI reports dealing with travel claim fraud by DoD personnel and with the theft of government property by DoD personnel. You can expect to see reports from these agencies dealing with the full range of criminal activity.

These reports are also unsolicited. How the information is reported to the CAF is a matter of individual Component practice, but you can expect to receive and adjudicate them on a regular basis.

CI Investigative Agencies

***INSCOM, NCIS
and AFOSI are
responsible for CI.***

Just as each Component has its own criminal investigative agency, each military department has its own counter-intelligence agency. Army's CI agency is the Intelligence and Security Command (INSCOM). Navy's (NCIS) and Air Force's (AFOSI) criminal agencies and CI for their respective departments. The other DoD agencies have agreements with one of the military agencies to give them support. The Component CI agencies investigate counterintelligence issues involving component personnel and information. (Note, however, that the FBI always has primary jurisdiction for these matters in the U.S., and will frequently work jointly with the Component on these investigations.)

Information relating to CI investigations may be reported to the CAF, provided, of course, that no CI operations are compromised by doing so.

***CI reports are
rare but
important.***

Although CI investigations, whether from the FBI or the Component agency, are probably the rarest reports that you'll see, they are also the most potentially important reports that you'll ever see. If you come across such a report, refer it immediately to your supervisor or a senior adjudicator

Other Federal Agencies

Besides the FBI and the DoD agencies, other Federal agencies will occasionally send reports which must be adjudicated under the CEP.

Sources of Information

Government Agencies



Other Federal agencies

State governments

Local governments

Foreign governments

6

Figure 6-9

Treasury and Justice are the most common non-DoD sources.

The Department of the Treasury has a number of agencies with investigative elements. The IRS, the Bureau of Alcohol, Tobacco and Firearms (ATF), and the Bureau of Customs all conduct investigations. These investigations usually deal with violations of Federal laws, such as tax fraud, illegal arms dealing and smuggling.

The Secret Service may provide information involving threats against the lives of the president, vice-president and other persons under their protection. In turn, DoD requires that any such threats be reported to the Secret Service. If you receive such information, you must determine immediately whether it has been reported. If not, the CAF must do so. The Secret Service is also responsible for investigating currency counterfeiting. When these investigations involve DoD personnel, they may be sent to the CAF for you to adjudicate.

The Department of Justice (DOJ) has a number of agencies besides the FBI which may be the source of information to be reviewed under the CEP. The Immigration and Naturalization Service (INS) and the

U.S. Attorney's Office are the DOJ agencies most likely to send you CEP information. Again, this information usually involves criminal matters, such as Alien Smuggling or other violations of Federal laws.

The Central Intelligence Agency may provide information relating to DoD personnel involved in CI issues under their authority.

Although the agencies discussed above are the CAF's most likely sources of information, virtually any Federal agency could send in reports for you to review and adjudicate under the CEP.

Foreign Governments also have personnel records that may be available to the adjudicator.

These reports also come to the CAF without being specifically requested.

State and Local Agencies

State and local criminal agencies may forward information.

In addition to agencies of the Federal government, state and local government agencies sometimes send information to the CAF. While this information is usually sent to the employing activity (who will then send it to the CAF), it may come directly to the CAF. State and local agencies usually provide criminal information from police departments, the courts and probation and parole offices.

Other Sources of Information

Private sources

Citizens

Organizations

Clinics

Anonymous



7

Other Sources of Information

Besides the various governmental sources, there are a number of other sources of CEP information for the CAF. Private citizens and government personnel may send information directly to the CAF. It's not unusual for a subject to provide derogatory information about other people when replying to an LOI or SOR. Or you may read a news report about a DoD affiliated person involved in some activity which raises questions about his/her loyalty, reliability or trustworthiness.

The information provided by most organizations and clinics is usually through the presentation of a release signed by the individual as part of an investigative process. There are times when information is provided by citizens as open sources (when they call to file a complaint for example) or anonymously (when they call to get someone to look into what they perceive as a "wrong").

One group of frequently checked private organizations that provides us information are educational institutions when they are presented with a release* signed by the individual. Some of these checks reveal that the individual does not have the degree that they claim to have.

***Releases (medical, education and credit/financial) are requested as part of many investigations. The DSS agent can request releases from the individual to resolve issue(s) in an SII.**

Information from some of these sources may not be complete enough to make a final decision about the subject's security eligibility. Most often, you'll use this information as the basis of a request for an SII from DSS

REMEMBER

The Continuous Evaluation Program, by its very nature, draws information from many sources. We have just discussed the most common sources of information coming directly to the CAF.

The FBI provides both criminal and CI information and is the most common source of information.

Each of the military departments has CI and criminal investigative agencies which are frequent sources of CEP information.

Other Federal agencies, such as Treasury and Justice, are occasional sources of information. Additionally, state and local agencies, foreign governments, and private individuals will sometimes send the CAF information which you'll review under the CEP. Additionally, state and local agencies, foreign governments, and private individuals will sometimes send the CAF information, which you'll review under the CEP

Review Exercise

1. A personnel security determination is an effort to assess the future _____ of an individual in terms of the likelihood of the individual preserving the national security.

2. In conjunction with the submission of PRs, _____ review an individual's SF 86 to insure that no significant adverse information of which they are aware that may have a bearing on subject's continued eligibility for access to classified information is omitted.

3. To protect classified information, the employee must know:

4. What are the four types of security briefings?

5. The continuous evaluation program recognizes that adverse changes occur in some persons' lives.
 - a. True
 - b. False

6. All members of DoD have the responsibility to report derogatory information on persons assigned to sensitive duties to the appropriate commander or security officer.
 - a. True
 - b. False

7. What are the two types of information provided by the FBI?

8. What are the criminal investigative agencies of the three military departments?

9. What are the CI investigating agencies of the three military departments?

10. What are the two non-DoD Federal agencies most likely to send the CAF information considered under the CEP?

11. Private individuals and the news media occasionally provide information to be reviewed under the CEP.

- a. True
- b. False

Solutions and References

1. **trustworthiness (Para 9-100, DoD 5200.2-R)**
2. **supervisors (Lesson 6, page 6-4)**
3. **How to protect it. (Lesson 6, page 6-11)**
4. **Initial, Refresher, Foreign Travel and Termination (Lesson 6, page 6-10)**
5. **a. True (Lesson 6, page 6-3)**
6. **a. True (Lesson 6, page 6-3)**
7. **Criminal and Counterintelligence (Lesson 6, page 6-14)**
8. **Army-CID, Navy-NCIS and Air Force-OSI (Lesson 6, page 6-15)**
9. **Army-INSCOM, Navy-NCIS and Air Force-OSI (Lesson 6, page 6-16)**
10. **The Departments of Justice and Treasury (Lesson 6, page 6-17)**
11. **a. True (Lesson 6, page 6-19)**
12. **FBI (Lesson 6, page 6-20)**