



**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>

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?

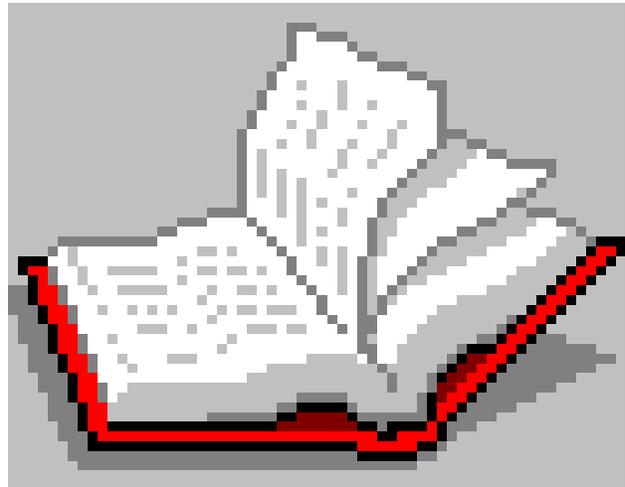
READING ASSIGNMENT

Assignment 2:

[Nov 98 Memorandum:](#)

Assignment 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)**