PERSEREC

Technical Report 00-4
November 2000

Security Clearances and the Protection of National Security Information Law and Procedures

Sheldon I. Cohen
Sheldon I. Cohen & Associates

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, California 93940-2497

Technical Report 00-4 **December 2000**

Security Clearances and the Protection of National Security Information: Law and Procedures

Sheldon I. Cohen
Sheldon I. Cohen & Associates

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
December 2000	Technical	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Security Clearances and the Protection of National Security Information: Law and Procedures	N00014-97-C0266
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Sheldon I. Cohen	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Sheldon I. Cohen 2009 N 14th Street, Suite #708 Arlington, VA 22201	PERS TR 00-4

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITOR'S ACRONYM(S)
Defense Personnel Security Research Center (PERSEREC) 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	PERSEREC
	11. SPONSORING/MONITOR'S REPORT NUMBER(S) PER-TR-00-4

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

PERSEREC undertook to sponsor the development of this report in order to make available in one place a readily understandable discussion of the complex laws and procedures that have been designed to protect National Security information. The report provides an authoritative compendium for lawyers, security officers and for managers of corporations who must deal with the legal and procedural aspects of security clearances and -not least-for government and contractor employees whose livelihoods depend upon their acquiring or maintaining security clearances.

15. SUBJECT TERMS

Security clearances, law and procedures;

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF REPONSIBLE PERSON
Unclassified					James A. Riedel, Director
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER *(Include area code)* 831-657-3000

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

Preface

The Defense Personnel Security Research Center undertook to sponsor the development of this report in order to make available in one place a readily understandable discussion of the complex laws and procedures that have been designed to protect national security information. The contents of the report are relevant to all employees and contractor personnel of the Department of Defense who require security clearances, and also to employees of federal agencies that deal with energy, intelligence gathering, and law enforcement.

Sheldon Cohen has provided in this report an authoritative compendium for lawyers, security officers, and managers of corporations who must deal with the legal and procedural aspects of security clearances and, not least, for government and contractor employees whose livelihoods depend upon their acquiring or maintaining security clearances.

James A. Riedel
Director

Acknowledgements

I want to acknowledge first the assistance of Dr. Theodore R. Sarbin, Project Manager, Defense Personnel Security Research Center (PERSEREC), whose advice, help, and understanding were immeasurable. The assistance is also acknowledged of many people from various federal offices who provided information that was not obtainable from published sources. Included among these are some individuals whose identities cannot be disclosed for security reasons.

Among those whom I can identify, and to whom I am indebted, are Richard A. Ferris, Associate Director for Investigations, U.S. Office of Personnel Management; a representative of the Central Intelligence Agency Office of General Counsel; Kim L. Hargrove, Esq., Assistant General Counsel, National Security Agency; Barry Dalinsky, Office of Safeguards and Security, U.S. Department of Energy; Robert R. Gales, Chief Administrative Judge, Defense Office of Hearings and Appeals; D. Jerry Rubino, Director, James P. Walker, Assistant Director, and Charles L. Alliman, Associate Director, Security and Emergency Planning staff, U.S. Department of Justice; Thomas N. Willess, Associate General Counsel, National Imagery and Mapping Agency; Steven Lewis, Security Specialist, Defense Security Service; and Michelle I. Walensky, Public Affairs Specialist, Federal Bureau of Investigation.

Grateful thanks go to Leon J. Schacter, Director, Defense Office of Hearings and Appeals and to Stuart Aly, Associate General Counsel, Defense Legal Services Agency, who reviewed the manuscript and whose comments were of invaluable help.

Finally, I wish to thank Dianne Johnson and Geneva Green in my office and Suzanne Wood at PERSEREC whose editorial assistance made this report possible.

Although all those named above provided great guidance and assistance, the content and opinions contained in this book are the responsibility of the author alone and to the best of my ability reflect the official positions of the departments or agencies reviewed. I have made an effort to provide up-to-date information, although I am aware that I am dealing in some sense with a moving target, for rules and regulations are changing constantly.

Table of Contents

Introduction

This report is intended to gather and analyze the law and procedure pertaining to national security clearances and the protection of national security information. It is written for lawyers practicing in this area of the law, for security officers and security managers of corporate government contractors dealing with classified information, and for government employees and contractor employees whose livelihoods depend on obtaining or keeping a security clearance. This field involves virtually everyone working for or doing business with the Department of Defense (DoD), the Department of Energy (DOE), and the various federal government agencies dealing with intelligence gathering or law enforcement.

The report is not about espionage and the laws dealing with espionage. That is an area of criminal law beyond this report's intended scope. Any deliberate intent to disclose national security information to unauthorized recipients, particularly to foreign recipients, is a matter for criminal investigation and prosecution by the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ). Nor is this report about intelligence gathering or the use of intelligence information that is within the province of the Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Imagery and Mapping Agency (NIMA), the Defense Intelligence Agency (DIA), and numerous other departmental intelligence agencies. Rather, this report is about the protection of national security information to prevent such information from being compromised and the granting of clearances and access to that information both to companies and to individuals. It concerns the processes and procedures used by the government to prevent the unauthorized disclosure of the nation's security information.

The agencies principally concerned with personnel security investigations are the Defense Security Service (formerly the Defense Investigative Service), the Office of Personnel Management, the FBI and the CIA for Sensitive Compartmented Information. Final clearance adjudications are principally the responsibility of the Defense Office of Hearings and Appeals for employees of government contractors, the Department of Energy for its employees and the employees of its government contractors; and for other government employees, the individual agencies' Adjudication Facilities and Personnel Security Appeals Boards.

The need for protecting a nation's secrets has been recognized from the earliest days of established government. In the United States the authority to do so has historically been based on the inherent war powers of the President under the U.S. Constitution. Besides those general powers, Congress, by statute, has vested in the President specific powers and means for protecting national secrets, most particularly since the end of World War II. Those statutes include the National Security Act of 1947 that established the CIA, and the National Security Agency Act of 1959 that established NSA. More recently enacted was the National Imagery and Mapping Agency Act of 1996, creating NIMA from a number of offices scattered throughout the government. That Act recognized and formalized the existence of the National Reconnaissance Office (NRO), which until then had been so secret that its very name could not be mentioned.

Presidents, through their Constitutional powers and the powers delegated by Congress, issued public Executive Orders and secret Directives, creating agencies and programs. The very existence of some of these programs is treated as a national secret. Systems for protecting secret information and for determining who will have access to that information have also been established by Executive decree. Yet even in protection of national security, probably the most important of the President's responsibilities, his power is not plenary. It is balanced with the other Constitutional imperatives of due process and equal protection for the citizens of this country. In that balance, however, the greater the need for secrecy and the more important the secret, the less weight is put on the individual's constitutional rights. Even in this critical area, the President's discretionary powers are not unfettered. He could not, for example, deny employment in a secret project simply because of a citizen's race. This country is hopefully long past the days when it interned its citizens simply because of their national origin, as was done to Japanese-American citizens in 1941. Although no one has a constitutional right to see classified information, if the government's reasons for denying access to classified information were shown to conflict with fundamental constitutional protections, the courts today would not refuse to consider and balance the conflicting constitutional interests.

One not familiar with the law of classified information might think that information might simply be classified "Secret" or "Not Secret"; or even "Confidential," "Secret," and "Top Secret." The system is far more complex. Information is categorized by its type, sensitivity, uses and origin. The right of an individual to see or use, i.e., to "access" a particular type or level of classified information always depends on his need to see the particular information. It also depends on his having been investigated and determined to be trustworthy and reliable. The degree of trustworthiness and reliability to which the person is held will increase, as will the intensity of their background investigation, as the sensitivity of the information to be available to them increases.

The type of due process afforded an individual whose clearance is threatened depends not only on the nature and degree of sensitivity of the information, but also on the employer. Contrary to common expectation, an employee of the United States Government, who would seemingly be considered more reliable because of the historical development of the law, has far fewer due-process rights than his industrial counterpart.

National security law is many faceted and somewhat arcane. Terms like "clearance" and "access" may at first blush seem the same. Nevertheless, they are significantly different, and that difference significantly affects an individual's or company's ability to deal with classified information. Personnel clearances and facility clearances are interrelated. Not infrequently, the mishandling of national security information will jeopardize both a company's right to hold classified information and an individual's security clearance. Someone not regularly involved in these issues might be bewildered when faced with a potential loss of a "clearance" or loss of "access." That loss could permanently deprive a person from working in the only field they know, or a company of a key employee or contract on which its very survival depends. At such times assistance should be sought from those people knowledgeable about the law and

procedure concerned with protecting national security information. It is to those people to whom this book is directed.

Note: While every effort has been made to make this book gender neutral, at times use of terms "he or she" or even the more cumbersome "he/she" tended to make the writing even more ponderous than it was already. For simplicity in such cases the pronoun "he" was used to encompass both male and female employees--with apologies for this shorthand.

CHAPTER 1

Constitutional and Statutory Authority for the Establishment of a National Secrecy System

The Government's Right to Protect Information

The right of the government to keep information secret is found explicitly in only two places in the U.S. Constitution. The first, Article I, Section 5, authorizes each House of Congress to publish a Journal of its proceedings, except for "such parts as in their judgment requires secrecy." The other, Article I, Section 9, requiring the publication of a statement of account of all public money "from time to time," has been interpreted to authorize keeping secret for a time certain expenditures for military or foreign relations.[1] Implicit, however, is the authority of the Executive Branch to keep information secret in carrying out its responsibilities in the areas of national defense and foreign relations.[2] This has been recognized from the earliest days of our country going back to military operations in the Revolutionary War.[3]

The Executive Branch exercised the power to protect national defense and foreign relations information without legal formality until 1947 when an executive order was first issued under President Truman.[4] This was followed by a series of four revisions, the first of which was issued in 1972 by President Nixon followed by three more updates under Presidents Carter, Reagan, and Clinton.[5] The executive order currently in effect, E.O.12958, closely resembles the Executive Order issued under President Carter, while the Reagan Order followed more generally the policies of President Nixon, reflecting the ebb and flow of the philosophies and policies of the political party then in power.[6]

The first Executive Order establishing standards for access to classified information by government employees was issued in 1953 by President Eisenhower.[7] A separate executive order providing procedures for appealing security clearance decisions by non-government, contractor employees was issued in 1960 by President Eisenhower and remains in effect today.[8] Most recently, President Clinton issued Executive Order 12968 in 1995 governing access to classified information by both government and nongovernment employees, and providing, for the first time, a government-wide procedure for appealing access decisions by government employees.

In addition to the inherent powers of the Executive Branch under the Constitution, its authority to keep information secret flows from five statutes: the Espionage Act,[9] the National Security Act of 1947,[10] the Atomic Energy Act of 1954,[11] the Counter-intelligence and Security Enhancements Act of 1994, amending the National Security Act of 1947,[12] and the Freedom of Information Act.[13] The National Security Act directs the Director of Central Intelligence to "protect intelligence sources and methods from unauthorized disclosure."[14] The Atomic Energy Act protects an entirely distinct category of information relating to the production of atomic weapons and nuclear materials.[15] The Counterintelligence and Security Enhancements Act of 1994 directs the President to

develop uniform requirements for background investigations and uniform standards for appeal of access denials.[16]

Executive Order 12958 "prescribes a uniform system for classifying, safeguarding, and declassifying national security information," i.e., information relating to "the national defense or foreign relations of the United States."[17] It establishes only three classification levels: Confidential, Secret and Top Secret.[18]

Certain information is considered so critical that, although not classified at a higher level, access to that information must meet more rigorous standards. Where the vulnerability of the information or the threat to it is exceptional, and normal criteria for determining eligibility for access to such information is deemed insufficient to protect that information, or when specifically required by statute, E.O. 12958 authorizes the Secretaries of Defense, State, and Energy and the Director of Central Intelligence to establish programs known as Special Access Programs to afford a greater degree of secrecy.[19] They are generally referred to as "SAPs." Some of these programs have been called "black" programs because their very existence or purpose is not publicly disclosed. Some are considered so sensitive that they are considered "waived" programs, and the existence of these is revealed only orally to the chairmen and certain staff members of key Congressional committees.[20]

Another category of protected information flowing both from inherent Presidential power and from statute is Sensitive compartmented information (SCI). That is information concerning intelligence, particularly the "sources and methods" of gathering intelligence. The legal bases for protecting this category of information are the National Security Act of 1947 and Executive Order 12333.[21]

The authority to protect information from disclosure includes not only the power to decide what information is to be protected, but who will have "access" to that information. Under Executive Order 12958, a person may have access to classified information only when a favorable determination of eligibility has been made by an agency head, when the person has signed a nondisclosure agreement and when the person has a need to know the information.[22] For SAP information, a standard of eligibility higher than normally established for the same level of classified information may be used.[23]

General guidelines for eligibility for access were established for the first time throughout the government in Executive Order 12968. They provide that an individual must be a U.S. citizen, of sound judgment and character, trustworthy, and free from potential foreign allegiances and coercion.[24] That executive order directed the Security Policy Board to carry out its requirements, and that Board has now developed uniform Adjudicative Standards binding on the Executive Branch that have been issued by the National Security Advisor.[25] Those uniform standards have been or are now being incorporated into each agency's regulations.[26] The uniform standards have also been incorporated by the Director of Central Intelligence in Director of Central Intelligence Directive 6/4 (DCID 6/4), the regulation controlling access to Sensitive compartmented information (SCI).[27]

Entirely separate systems have been established to determine eligibility for access by contractor employees and by government employees, and for eligibility for access to SAP and SCI information. The standards, investigatory methods, and procedures are discussed in detail in Chapters 4, 5, 7, and 8.

The determining of security accesses and clearances is a major government program that has become its own cottage industry. Whole agencies have been created that do nothing but investigate and make such determinations. The cost to the government and industry of protecting classified national security information was reported for 1989 to be $13.8 billion. By 1995, primarily due to the end of the Cold War, it was reported to have dropped to $5.6 billion.[28]

An Individual's Rights in Relation to the Protection of Classified Information

Although the President has plenary powers under the Constitution to protect the national security and conduct foreign relations, those powers do not automatically overcome the rights of association; freedoms of speech, religion, liberty and due process; and the equal protection of the law guaranteed to citizens under the Fifth and Fourteenth Amendments of the Constitution.[29] The courts have balanced these potentially countervailing interests, and though considerations of national security weigh very heavily on the scales, an individual's interest in employment and to be free from discrimination cannot be ignored.[30] The process that is due and the equality of protection afforded always depend on the issues at stake. In general, however, the courts will not interfere with the Executive Branch's discretionary judgments of eligibility.[31] Colorable constitutional claims and whether an agency has followed its own procedures are reviewable by the courts unless Congress has clearly expressed its intent to preclude judicial review of constitutional claims.[32] Moreover, the Supreme Court has said that any attempt by Congress to "deny any judicial forum for a colorable constitutional claim would raise serious constitutional concerns."[33]

While the Executive Branch's determinations are virtually unchallengeable, they are not without some limits. The Supreme Court in *Dept. Of Navy v. Egan* reiterated that the courts have, in the area of national security, "shown utmost deference to Presidential responsibilities" and "have been reluctant to intrude" in national security affairs, but its decision a few months later in *Webster v. Doe* leaves the door open for challenge, based on a violation of Constitutional right. Denial of a clearance in this day because of discrimination for race, religion, or national origin would be unthinkable.[34] It is far from certain, if there was a direct confrontation of these values, what the outcome would be in view of the courts' upholding of the Executive Branch's power to exclude lesbians and male homosexuals from the military.[35] Fortunately, those issues have been mooted by Executive Order 12968 that prohibits discrimination "on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information."[36]

Because of historical anomalies in the case law, two procedural systems have evolved for determining eligibility for access to national security information. One system exists for employees of government contractors, for whom a full administrative

hearing is allowed, with the right to present and cross examine witnesses, and another for government employees who have no such rights.[37] The Department of Energy, under the authority of the Atomic Energy Act, has combined these into a single system granting the full body of due process rights to both classes of employees.

In *Greene v. McElroy,* a 1959 case, the Supreme Court held that an employee of a defense contractor, whose loyalty was questioned, had the right to be shown the government's evidence against him and the opportunity to demonstrate that it was untrue.[38] The Supreme Court's later pronouncement in *Dept. Of Navy v. Egan* did not require any administrative hearing for government employees, holding that there is no inherent right to a security clearance, and that the Executive Branch has the discretionary right to grant access to classified information.[39] While there is no logical way to reconcile these two decisions, the gap has been partially closed by later Executive action. President Clinton, by Executive Order 12968, has provided a truncated appeals process for government employees or applicants for employment that requires that they be presented with the reasons for denying their eligibility for access, and be allowed an opportunity to make a written and oral presentation to present evidence why they should have access.[40] While not formalized to the degree of having a hearing on the record with the right to cross-examine the government's witnesses, the procedure allowed by the executive order is a degree of due process that, in all likelihood, meets Constitutional requirements, and a degree that would be sustained by the courts.

While procedures, more or less elaborate, are available to challenge adverse determinations of a person's *eligibility* for access, the determination of a person's *need* for access is, under the executive order, discretionary and conclusive with the Executive Branch.[41] Frequently, the line between these requirements becomes blurred. Under the "need" determination, people in the past have been denied access to SCI and Special Access programs without ever knowing that they have been investigated or found to be unsuitable. Today, DCID 6/4 has been revised to require that people be notified of the reasons for denial of access to SCI with a limited right to appeal. That directive does not, however, affect SAPs.

If a government employee is denied access to a SAP program without notification, that presumably would have no effect on his employment because so long as the employee held a security clearance, he would not lose his job. But for a contractor's employee, denial of SAP access would mean that he would not be hired for a job requiring SAP access, or would be laid off when work not requiring SAP access became unavailable. The contractor employee would not be the wiser, because he would never have been told that he was considered and rejected for employment in a SAP or "black" program.

The Standardization of the Industrial Security Program

During the Cold War years of the 1950s through the 1970s, the nation's industrial community grew to meet the government's need for military, intelligence, and nuclear products. Each government agency at that time developed its own requirements and standards for protecting its national security information. By the end of the 1980s, the exces-

sive cost to both industry and the government of multiple standards and requirements became overwhelmingly apparent. It was recognized that not only was there a plethora of government personnel security programs, but there were numerous overlapping industrial security programs, each with differing requirements for protecting classified information and each with differing standards for physical security of facilities. In April 1990, the President directed the National Security Council to explore the development of a single, integrated industrial security program that might result in cost savings and improved security protection. Before the end of that year the Secretaries of Defense and Energy, and the Director of Central Intelligence submitted a report recommending the establishment of a National Industrial Security Program (NISP).[42] Their report found that there were 21 Departments and agencies, each with its own industrial security program. It found that in DoD alone there were 47 different standards, manuals, and directives supplementing the basic executive orders and legislation, creating a significant burden on industry and government. It reported that more than 25,000 people had multiple background investigations conducted by the various agencies with which they dealt. The cost to industry was $120 million a year in added administrative costs and employee downtime while waiting for the additional clearances for employees who had already been cleared in other areas.[43] That added cost was, of course, passed on to the government through higher prices. The report found that standardization of requirements could reduce duplication by at least 20 percent.

The 1990 Report recommended the establishment of a National Industrial Security Program under the direction of the DoD, leaving to the Secretary of Energy the authority to protect nuclear materials. It also recommended leaving to the Director of Central Intelligence the authority to protect sensitive compartmented information, i.e., intelligence sources and methods, because of their need for extraordinarily stringent controls. Special Access Programs (SAPs) were also considered a special need. From those recommendations came a government-wide consolidation of industrial security requirements for physical security, known as the National Industrial Security Program (NISP). It also resulted in the development of a standardized background investigation that became known as the Single Scope Background Investigation (SSBI).

Based on that report, an interagency task force was established in December 1990 to develop a National Industrial Security Program. It was given six months to turn around 40 years of institutional evolution. The recommendations of that task force, which included opinions and ideas from industry panels, and from the American Bar Association on personnel security issues, became the basis for the simplification of the entire classified information program. Ultimately, from that report came uniform standards for determining a person's eligibility for access to classified information, and uniform appeal procedures if a security clearance or access was denied or revoked.

The first effort to consolidate the clearance process was the issuance of National Security Directive 63, *Single Scope Background Investigations,* in 1991 that set minimum standards for Top Secret clearances and that required each agency to recognize the background investigations of other agencies. Its purpose was to eliminate redundant and costly investigative practices used throughout the Executive Branch.[44] That consolidated investigation, known as the SSBI, replaced the Background Investigation (BI) required

for access to Top Secret information, and the Special Background Investigation (SBI) required for Sensitive compartmented information.[45] The SSBI required a personal interview of the subject, law enforcement and credit checks, and interviews with people knowledgeable of the subject's lifestyle and background covering a 10-year period. It allowed agencies to exceed those standards to address issues unique to those agencies. Some agencies such as the CIA, the NSA, the FBI and the Treasury Department were allowed to continue to use polygraphs to screen employees and applicants because of the nature of the national security information with which they dealt.[46]

The next step in the consolidation was the issuance of Executive Order 12829 on January 6, 1993, formally establishing the National Industrial Security Program. The program was to serve as a single, integrated, cohesive industrial security program to protect classified information. That executive order directed the National Security Council to provide overall policy direction, directed the Information Security Oversight Office (ISOO) to oversee the implementation of the executive order, and directed the Secretary of Defense to issue a National Industrial Security Program Operating Manual to prescribe the specific requirements for safeguarding classified information by contractors, licensees, and grantees. The Secretaries of Energy and the Nuclear Regulatory Commission were given responsibility for the portion of the manual dealing with nuclear energy, and the Director of Central Intelligence was made responsible for the portion dealing with intelligence sources and methods, i.e., sensitive compartmented information.

The National Industrial Security Program Manual (NISPOM) was issued in October 1994, and a supplement dealing with SAPs, sensitive compartmented information (SCI) and critical restricted data (RD) was issued in December 1994.[47] It replaced the Department of Defense Industrial Security Manual for Safeguarding Classified Information.

The need for further consolidation remained apparent. In 1993, because of the fragmented personnel security system, the Secretary of Defense and the Director of Central Intelligence appointed a Joint Security Commission to study and make recommendations for a simplified, more uniform, and more cost-effective system. The Commission issued its report, *Redefining Security,* in February 1994 addressing problems not only in personnel security, but also in physical security, classification management, and information systems security.

Congress acted swiftly to accept many of the Commission's recommendations. In October 1994 it amended the National Security Act of 1947 to require the President to establish standards and procedures to govern access to classified information binding on all departments, agencies, and offices of the Executive Branch.[48] It was intended that those standards and procedures create uniform minimum requirements governing the scope and frequency of background investigations and provide uniform minimum standards for appealing adverse access determinations. The law required that employees in the Executive Branch whose access to classified information was threatened with denial or termination be so advised and be given an adequate opportunity to respond to any adverse information before a final agency decision. The purpose of the legislation was to provide a procedure that would ensure that security determinations were not made based

on inaccurate or unreliable information because of their impact on the careers and livelihoods of the individuals concerned, and the possibility of depriving the government of the services of valuable employees.[49]

As a result of this legislation, President Clinton signed Executive Order 12968, *Access to Classified Information,* on August 2, 1995 that required: (a) reciprocal acceptance by agencies of each other's security investigations, (b) a common set of adjudicative guidelines for determining eligibility for access to classified information, (c) a common set of investigative standards for background investigations, and (d) minimum review procedures for those whom it had been determined did not meet the standards for access to classified information. These standards and procedures applied not only to government and contractor employees but also applicants for employment. It did not supplant the greater appeal procedures for contractor employees. The Executive Order directed the Security Policy Board to carry out its requirements.[50] It supplemented but did not replace National Security Directive 63 that had previously established the investigative standards for the Single Scope Background Investigation. The Security Policy Board developed uniform adjudicative and investigative standards that were approved by the White House on March 24, 1997.[51] They are binding on the entire Executive Branch and have been or are being incorporated in each agency's regulations.[52]

The remaining act of unification and standardization in the field of protecting national security information was the issuance of Executive Order 12958, *Classified National Security Information,* on April 17, 1995, establishing a uniform system for classifying and declassifying national security information. The executive order directed the Information Security Oversight Office (ISOO) to oversee compliance with the order and created the Interagency Security Classification Appeals Panel to resolve classification disputes arising under the order.

In the view of many, the task of consolidation and simplification is far from complete. In March 1997, the Commission on Protecting and Reducing Government Secrecy, a bipartisan commission created by Congress to review matters related to classified information and security clearances, issued its report.[53] The report contained a number of significant recommendations among which were: (a) enactment of a statute that would state the principles of what may be declared secret, (b) creation of a national declassification center to coordinate the declassification of information, (c) establishment of an Executive Branch office responsible for classification and declassification practices, (d) requirement that officials who initially classify information consider the costs and benefits of secrecy as a factor in keeping something secret, (e) requirement that the Director of Central Intelligence issue guidelines for determining what intelligence sources and methods are to be kept secret, (f) further standardization of the security clearance procedures, and (g) greater attention to the threat to automated information systems.

On May 7, 1997, S. 712, dubbed the Government Secrecy Reform Act, was introduced by Senators Daniel Moynihan and Jesse Helms to enact the consensus recommendations of the Commission.[54] Hearings were held and a report issued by the Senate Committee on Governmental Affairs. However, no further action was taken in the 105th Congress.[55] The bill was reintroduced in the 106th Congress on January 19, 1999 by

Senators Moynihan and Helms.[56] At the time of this writing, no legislation has been enacted to carry out any of these recommendations, nor has the Executive branch taken any steps to carry them out.

CHAPTER 2

Type and Scope of Background Investigations

Background of the Present System

Before employees or applicants for employment in government or industry can have access to national security information, they must undergo a background investigation to determine whether they are sufficiently trustworthy to hold a security clearance. The length and complexity of the investigation varies depending on the type of clearance required and the nature and sensitivity of the information being protected. Confidential, Secret, and Top Secret clearances each have different investigative requirements, as do "Q" and "L" accesses for the Department of Energy. Access to Sensitive Compartmented Information (SCI) and to special access programs has even more stringent investigative requirements. The type of investigation required and the scope of each investigation are discussed in this chapter.

Because over the years each agency had developed its own requirements and its own unique forms, frequently requiring information not required by other agencies, it was decided at the highest government levels to consolidate and simplify the clearance application process. As a first step, the White House in 1991 issued National Security Directive 63, which established standards for a single background investigation to be used throughout the government for Top Secret clearances.[57] Those unified standards are known as the Single Scope Background Investigation (SSBI). That Presidential action was overtaken by legislation in 1994 requiring the Executive Branch "to establish uniform minimum requirements governing the scope and frequency of background investigations of all employees in the Executive branch of Government" requiring access to classified information.[58] While that statutory requirement is binding on all departments, agencies and offices of the Executive Branch of government, it does not apply to contractor employees.

The requirements of the statute were carried out by Executive Order 12968 on August 2, 1995, which directed the Security Policy Board to develop a common set of adjudicative standards for background investigations for access to classified information.[59] Agencies were allowed under the Executive Order to use any lawful investigative procedure to resolve issues that might arise during an investigation. The statutory mandate was further carried out when the Security Policy Board published the *Uniform Investigative Standards* on March 24, 1997.[60]

The Executive Order and the Security Policy Board's Uniform Standards apply to all U.S. Government civilian and military personnel. Although not required by statute, they also apply to consultants, contractors and their employees, licensees, and grantees of the government.[61] They establish standards for collateral clearances, i.e., Confidential, Secret, and Top Secret, and for SCI and Special Access Programs access determinations. "Q" and "L" accesses under the Atomic Energy Act are also covered. The Standards allow for enhanced investigative requirements for certain Special Access Programs if they are specifically approved under Executive Order 12958.[62]

The Uniform Standards require that investigations meeting the standards for a given level of clearance must be mutually and reciprocally accepted by all agencies. They also provide that if a person who has less than two years' break in service is reemployed, a reinvestigation will not be required unless it appears that the person no longer satisfies the standards.

Scope of Clearance Investigations

The Security Policy Board has established three investigative standards. The first standard is for Confidential, Secret, and "L" clearances and includes all Secret level Special Access Programs (except those with "enhanced requirements").[63] The second standard is for Top Secret and "Q" clearances, including those in SCI and Top Secret Special Access Programs. The third standard is for reinvestigations of persons already cleared.[64] All investigations include a National Agency Check as a minimum.

National Agency Check (NAC)

The National Agency Check consists of a review of: (a) the FBI's investigative and criminal history files including a fingerprint search, (b) Office of Personnel Management (OPM)'s Security/Suitability Investigations Index (SSI), (c) the Department of Defense Defense Clearance and Investigations Index (DCII), and (d) such other national agency records as are appropriate to the individual's background.[65] Those other agencies may include the Immigration and Naturalization Service for records of citizenship, the State Department, the CIA, the Treasury Department and the Department of Defense for military personnel records. Any other federal agency's records may be checked where appropriate to the investigation.[66] For an NAC, the applicant must submit a Standard Form 86 (*Questionnaire for National Security Positions*), along with all releases and a fingerprint card.

National Agency Check with Local Agency and Credit Checks (NACLC)

A National Agency Check with Local Agency and Credit Check inquiries includes, in addition to the National Agency Check requirements: (a) a financial review including a credit bureau check covering the places where the applicant has resided, worked or gone to school for the previous seven years; (b) a check with law enforcement agencies where the applicant has lived, worked, or attended school within the last five years; and (c) independent confirmation of date and place of birth. The investigation may be expanded if necessary.[67]

Single Scope Background Investigation (SSBI)

The requirements for a Single Scope Background Investigation were established in National Security Directive 63. These requirements have been incorporated in the Uniform Investigative Standards adopted by the Security Policy Board.[68]

The scope of the SSBI is the prior 10 years or to age 18 of the applicant, whichever is less. An investigation may be expanded, as necessary, to resolve employment issues and standards unique to individual agencies. Investigative requirements are:

(a) completion of SF 86; (b) a National Agency Check on the applicant with a fingerprint check; (c) a National Agency Check of the subject's spouse or cohabitant without a fingerprint check; (d) verification for naturalized citizens of U.S. citizenship of the applicant and of his or her immediate family members; (e) independent verification of birth, education, employment history, and military history; (f) interviews with four references at least three of which have been independently developed, and with any former spouse divorced within the previous 10 years; (g) confirmation of present and past residences and interviews with neighbors; and (h) review of public records concerning the applicant for bankruptcies, divorces, and civil or criminal actions. A personal interview of the applicant is required in all cases, conducted by trained investigative, counterintelligence or security personnel. Additional interviews may be conducted to resolve significant information inconsistencies. For departments or agencies, where authorized, the personal interview may include a polygraph examination.[69]

Confidential, Secret, and "L" Clearance Investigations

Confidential, Secret and L clearance investigations, require, in addition to a National Agency Check, a local agency and credit check (NACLC).[70] The investigation may be expanded if necessary. Reinvestigations of persons holding Secret and "L" clearances must be conducted at least every 10 years — for Confidential, it is every 15 years.

Top Secret and "Q" Clearance Investigations

The Single Scope Background Investigation is used for initial investigations for access to Top Secret, including Top Secret Special Access Programs (SAPs), and for access to Sensitive Compartmented Information (SCI). It is also used for "Q" access authorizations under the Atomic Energy Act.[71]

The SSBI may be expanded to resolve issues where the applicant has resided abroad, or has listed foreign travel or connections with possible subversive organizations. Medical records will be reviewed if the applicant lists a history of mental or nervous disorders or addiction or abuse of drugs or alcohol. In that case, interviews with relatives, psychiatrists, psychologists, and other medical and law enforcement professionals may be required.

A preemployment polygraph is required only for those agencies for which it has been approved. These include the FBI, the CIA, the National Security Agency, the Defense Intelligence Agency, and a limited number of positions in the Department of Justice and in the Drug Enforcement Agency. It may be used in connection with investigations or reinvestigations by other agencies to resolve issues that arise.

Periodic Reinvestigations (SSBI-PR)

Periodic Reinvestigations are required for Top Secret accesses, including those dealing with Special Access Programs and Sensitive Compartmented Information, and for "Q" access authorizations.[72] The investigation, known as a Single Scope Background Investigation - Periodic Reinvestigation (SSBI-PR), must be conducted at least every five years. The requirements are the same as those for an initial SSBI with the following

exceptions: (a) a National Agency Check is not required on a spouse or cohabitant if already completed in connection with a prior investigation, (b) no further review of education is needed, (c) employment is verified only since the last investigation, (d) only two references and two neighbors must be interviewed, and (e) the Treasury Department's financial data bases are checked for unusual or illegal financial transactions covering the period while the person held a security clearance.

Temporary Eligibility for Access

In exceptional circumstances where official functions must be performed before the completion of the investigation and adjudicative process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. Where such eligibility is granted, the initial investigation will be expedited.[73] If unfavorable information is identified during the investigation, the agency granting the temporary access may revoke it at any time.[74]

At a minimum, temporary access at the Confidential, Secret, and "L" levels requires the completion of a Personal Security Questionnaire, SF 86, a favorable review of the form and submission of a request for an expedited National Agency Check with Local Agency Checks (NACLC). The minimum required before a temporary Top Secret and "Q" access is allowed is favorable review of the SF 86 and submission of a request for an expedited SSBI. For temporary SCI access, and for persons who have not previously had a favorable security investigation, there is also required a favorable review of the FBI criminal and investigative records, of OPM's Security/Suitability Investigations Index (SII), and of the Defense Clearance and Investigations Index (DCII). Agency heads may establish additional requirements for temporary access based on the sensitivity of the particular classified information involved, but those requirements may not exceed the common standards for background investigations established by the Security Policy Board. Temporary access is not reciprocal and is valid only at the agency granting it. However, another agency may agree to accept it.[75]

The Personal Interview

Questions asked during a personal interview must have relevance to the security determination. Questions concerning religious beliefs and affiliations, beliefs and opinions regarding racial matters, political beliefs, and affiliations of a non-subversive nature are prohibited.[76] Also barred are questions relating to opinions regarding the constitutionality of legislative policies and questions concerning affiliations with labor organizations and fraternal organizations.

Department of Defense regulations require department investigators, including those from the Defense Security Service, to be prepared to explain the relevance of their inquiries. The regulations do not permit inferences to be drawn from a refusal to answer a question for which relevance has not been established.[77] Interviewers are instructed not to offer any opinion regarding the relevance or significance of any answers given to eligibility for access to SCI. Information developed during the interview is required to be kept in personnel security channels and access to that information is limited to those with a

need to know.[78] The Office of Personnel Management Manual for Personnel Investigations gives its investigators the same direction.[79]

Sensitive Position Investigations

Positions not requiring access to "national security information" can still have a material adverse effect on the national security. Such positions are designated as Sensitive positions for which a full field investigation is required.[80] OPM has defined four levels of sensitivity: (a) Special-Sensitive - those positions with a "potential for inestimable damage to the national security," (b) Critical-Sensitive - those with a potential for "exceptionally grave damage, (c) Noncritical-Sensitive—those with a "potential of damage or serious damage," and (d) Non-Sensitive—those that are "potentially prejudicial."[81]

With respect to national security classifications, Critical-Sensitive includes access to information classified at the Top Secret level, Noncritical-Sensitive includes access to Secret information, and Confidential and Non-Sensitive apply to all other positions. In addition to positions with access to national security information, Sensitive positions include those that are policy making or policy determining, investigative, fiduciary, or involve the public trust or public contact. Positions that have a major responsibility with computer systems, or which have access to computer systems so as to be able to cause major damage, are also considered Sensitive positions.[82]

Background investigations for Sensitive positions in the Department of Defense are covered by DoD's Personnel Security Program Regulation, 5200.2-R. Investigative requirements for such positions are described in Chapter 3 of the regulation. OPM conducts investigations for sensitive positions in non-Defense agencies, except the FBI and the CIA. Investigative requirements are described in the *Federal Personnel Manual*, Chapter 732.[83]

CHAPTER 3

Security Clearance Investigations by the Defense Security Service

Organization of the Defense Security Service

As a result of a defense reform initiative in 1997, the Defense Investigative Service (DIS) was renamed the Defense Security Service (DSS).[84] DSS investigators are responsible for conducting personnel security investigations (PSIs) to carry out the DoD Personnel Security Program.[85] DSS also administers the National Industrial Security Program on behalf of DoD. (See Chapter 11.)[86] DSS employs approximately 2,500 people consisting of approximately 1,200 Special Agents located throughout the United States and Puerto Rico and approximately 200 Industrial Security (IS) Representatives also located in offices throughout the United States; in Brussels, Belgium; and in Mannheim, Germany.[87]

Under the PSI Program, DSS has responsibility for conducting PSIs on DoD military, civilian and contractor personnel, and employees of other organizations performing research and development for DoD. If DSS encounters evidence of espionage or subversion, the matter must be referred to a military department counterintelligence agency or the FBI.[88] Allegations of possible criminal conduct arising during a personnel security investigation must be referred to the appropriate Department of Defense criminal investigative agency or civilian jurisdiction.[89] DSS may not refer allegations of private consensual sexual acts between adults to law enforcement agencies or military departments (other than a departmental central adjudication facility (CAF) for security clearance adjudications) except if those acts are openly in public view, for compensation, aboard a military vessel or aircraft, or with a subordinate while on active military or reserve duty. Information about a person's sexual orientation, or that he or she is a homosexual or bisexual, may not be reported for any purpose except to a CAF for an adjudication of whether that person would be subject to blackmail if trying to conceal that information.[90]

In addition to its investigative functions, DSS maintains the Defense Clearance and Investigations Index (DCII), one of the central repositories of information on security clearances files for government and industry personnel. The DCII is more fully discussed in Chapter 9.

Personnel Security Investigations

DSS conducts about 40 percent of the personnel security investigations performed each year by the Federal government. The Office of Personnel Management Investigations Service also does about 40 percent, and the FBI and the CIA each do about half the remainder.[91] DSS's personnel investigations are conducted both by its Special Agents who are government employees, as well as by private contract investigators, as is done by other government agencies.[92]

DSS conducts more than 150,000 personnel security investigations annually, which are used by DoD adjudicative facilities to determine an individual's suitability to enter the armed forces, access classified information, or hold a sensitive position within DoD. In addition to initial investigations, DSS conducts Periodic Reinvestigations (PRs) to determine if it is still consistent with national security standards for a subject to continue to have access to Classified information or to be retained in a sensitive position. The scope and frequency of a PR depends on the initial investigation conducted and the type of information to which the subject will have access or the sensitive nature of their position. PRs may be initiated at any time following completion of, but not later than 5 years for Top Secret, 10 years for Secret, and 15 years for Confidential.

As a result of policy changes affecting the frequency and scope of PRs and the upsurge in information technology positions in government and industry requiring clearances, there is a significant backlog of PRs within DoD resulting in an increased investigative workload within DSS. In order to meet requirements, DSS has initiated an approach to augment its investigative workforce with the use of private industry contractors and military reservists. Additionally, in a memorandum dated September 19, 1999, the Assistant Secretary of Defense (C3I), mandated that all investigations for DoD civilian personnel, except for overseas investigations, be conducted by the Office of Personnel Management beginning October 1, 1999. This arrangement will be reviewed at the end of FY00 and each subsequent fiscal year until the Periodic Reinvestigation backlog is resolved. Presidential appointees in DoD who require security clearances are investigated by the FBI. Although the National Security Agency and the National Reconnaissance Organization are "carve outs" from DSS's investigative authority, DSS also does the investigations for all but the most sensitive positions at NSA.[93]

Contractor employees in private industry who require security clearances are investigated by DSS under the Industrial Security Program, not only for DoD but also for 21 other government agencies.[94]

A personnel security investigation must be requested by electronically submitting a DD Form 1879 and a *Questionnaire for National Security Positions*, Standard Form 86, completed by the person for whom a clearance is required. A request may be submitted by a defense agency, the security officer of a contractor or by a government entity. The requester must certify that the individual for whom a personnel security investigation is requested is assigned to a job that requires access to classified information.

Once a request is received, case analysts at the DSS Personnel Investigations Center (PIC) scope the investigative leads to various DSS field offices throughout the country. Investigations are conducted according to the policy outlined in the DoD 5200.2-R (Personnel Security Program) and the procedures in the DSS Personnel Security Investigative Manual, *DSS Manual 20-1-M*.[95] Following completion of the investigation, the investigative results or Report for Adjudication is forwarded to the appropriate DoD Central Adjudicative Facility (CAF).

DSS uses polygraphs during security clearance investigations when unresolved issues have arisen during the investigation. It does not do counterintelligence investigations

or clearance investigations that require a polygraph as part of the initial clearance process. The polygraphs may be used as a personnel security screening measure only in those limited instances authorized by the Secretary of Defense in DoD Directive 5210.48.[96] Participation by the individual being investigated in a polygraph for a "collateral," i.e., Confidential, Secret or Top Secret clearance, is voluntary, and no inference may be drawn simply from the person's refusal to take one. However, if issues remain that have not been resolved in the individual's favor, the investigation will go forward in that status, and inferences will be drawn against granting a security clearance based on those unresolved issues. The use of polygraphs during security investigations is more fully discussed in Chapter 8.

Pursuant to the Privacy Act of 1974, most of the information contained in the DSS investigative file is available to the Subject, but only after the investigation is completed. Some material such as confidential source information, third agency information, medical information which a physician has determined would be harmful if released to the Subject, and information which would constitute an unwarranted invasion of the personal privacy of another person (e.g., spouse NAC information) may be exempt from the mandatory disclosure provisions of the Privacy Act and therefore may not be released to the Subject. A request for investigative files should be directed in writing to the Defense Security Service, Privacy Act Branch, P.O. Box 46060, Baltimore, MD 21240-6060. The request should be signed by the Subject of the file, notarized and contain the Subject's social security number, date of birth, and address where the file is to be mailed.[97]

The adjudicative agency for contractors is the Defense Office of Hearings and Appeals. For members of the military or civilian employees of the DoD, the investigation is referred to their respective CAFs.[98] The decision whether a person is sufficiently trustworthy to hold a clearance is initially made by those offices. If the decision is unfavorable, an appeal by a military member or government employee may be taken from the CAF to the Personnel Security Appeals Board of the Department concerned, or for a contractor employee to the Defense Office of Hearings and Appeals for a final decision (See Chapters 6 and 7).

Facility Clearances

The Industrial Security Program includes the Defense portion of the National Industrial Security Program; the Arms, Ammunition, and Explosives (AA&E) Program; and the Critical Infrastructure Protection (CIP) Program. The National Industrial Security Program (NISP) was established to ensure that private industry and colleges/universities properly safeguard classified information in their possession while performing on U.S. or foreign government classified contracts or research and development. The AA&E Program provides protection for conventional arms, ammunition, and explosives in the custody of DoD contractors. The CIP provides for the protection and assurance of Department of Defense Critical Assets and Infrastructures in the private sector throughout the world to support national security preparedness responsibilities during peace, crisis, and war.

Under the NISP, DSS is responsible for granting facility clearances and for ensuring the protection of classified information in industry. A facility clearance is an administrative determination that a company is eligible for access to classified information or for an award of a classified contract.[99] Facility clearances are more fully discussed in Chapter 11. Periodic reviews of cleared companies are accomplished by DSS Industrial Security Specialists who are trained in the requirements of the NISPOM.

Investigations of Foreign Ownership, Control, or Influence (FOCI)

As part of the facility clearance process and continuing eligibility assessment, DSS is responsible for determining whether U.S. companies are under foreign ownership, control, or influence (FOCI). DSS also prescribes responsibilities in FOCI matters and outlines security measures that may be considered to negate or reduce the FOCI to an acceptable level. A U.S. company is considered to be under foreign ownership, control, or influence when a foreign interest has the power, direct or indirect, whether or not exercised, to direct or decide matters affecting the management or operations of the company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts. The factors outlined in paragraph 2-302a, *National Industrial Security Program Operating Manual*, are considered in the aggregate when determining if a U.S. company is under FOCI.[100] A U.S. company determined to be under FOCI is ineligible for a facility security clearance, and a U.S. company with an existing facility security clearance will have its clearance suspended unless security measures are taken to mitigate the FOCI to an acceptable level. FOCI investigations are more fully discussed in Chapter 11.

CHAPTER 4

Security Clearance Investigations by the Office of Personnel Management

Jurisdiction and Operations of the Office of Personnel Management (OPM)

OPM's Office of Personnel Management Investigations Service now conducts about 45,000 national security investigations annually, which are 40 percent of the total personnel security investigations for the federal government.[101] It also conducts nonsecurity "suitability" investigations and other types of investigations related to OPM's role in personnel management and debt collection.[102]

OPM began conducting personnel security investigations in 1953 as a result of the authority given it by Executive Order 10450. In 1954, it obtained additional authority to conduct personnel security investigations under the Atomic Energy Act for the Department of Energy and the Nuclear Regulatory Commission. OPM currently is responsible for personnel security investigations, including Single Scope Background Investigations (SSBIs), for most of the non-Defense civilian government agencies. It also does investigations for those DoD civilian employees requiring no higher than a National Agency Check (NAC) with local agency checks and credit (NACLC) investigations for Secret or Confidential clearances.

Until 1996, the Investigations Service conducted its investigations with a government staff of about 750 personnel. Now, all of its investigations are contracted out to USIS, Inc., a private corporation formed with government approval, comprised of former OPM staff investigators. The Investigations Service, now with a staff of about 50, manages and does quality assurance checks on the investigations done by USIS, Inc. The Investigations Service operates on a revolving fund basis, charging its customer agencies for the cost of its investigations. These currently run from about $60 for a National Agency Check to $2,995 for a Single Scope Background Investigation with rush service.[103]

Investigations of contractor employees under the Industrial Security Program are conducted by OPM only for the Department of Energy and the Nuclear Regulatory Commission, the remainder being done by the Defense Security Service for the Department of Defense and for 20 non-DoD agencies. OPM investigates but does not "adjudicate," i.e., determine an individual's eligibility for a security clearance, except for its own employees.[104] Once an investigation is completed by USIS, Inc. and accepted by OPM, the information that has been collected on an individual is forwarded to the agency that has requested the investigation. It is that agency which "adjudicates," i.e., evaluates the information and determines whether to grant a security clearance. Adjudications of government employees and appeals of those adjudications are performed under the provisions of Executive Order 12968. (See Chapter 6.) Adjudications and appeals of contractor employees' clearances are in accordance with the processes provided by Executive Order 10865. (See Chapter 7.)

OPM maintains the Security Investigations Index (SII) which is a listing of all security investigations conducted by that or any other civilian agency. (See Chapter 9.) It is now starting another data base that will list all security clearances granted or revoked throughout the civilian agencies of the government, information not included in the SII. The new index appears to overlap the DCII maintained by the Defense Security Service.

OPM characterizes all investigations on a scale of "A" through "D," "A" cases being those with no substantial issues, and "D" cases being those with very substantial issues of concern. The cases are rated based upon a matrix of standards established by OPM that it calls "issue codes" and "seriousness codes."[105] Code ratings are assigned by the investigator to any questionable conduct relevant to the uniform Adjudicative Standards, the ratings are tallied and the case is assigned an overall rating. If a completed investigation is coded "D" when forwarded by OPM to the requesting agency for adjudication, the agency must report back to OPM within 30 days of what action it has taken. If the agency takes no action, OPM may revoke the employee's eligibility for government employment, based on a determination of "unsuitability."

The number of investigations done by OPM, and the results of those investigations has remained remarkably consistent from year to year.[106] Noteworthy is how many contain "actionable" issues. Less than half the Single Scope Background Investigations, Background Investigations and Limited Background Investigations show no "actionable" issues. For Periodic Reinvestigations of those people already holding security clearances, slightly more than half show no actionable issues. Individuals having National Agency Check with Inquiries investigations for the lowest level clearances fared the best with the least number of issues of concern.

In fiscal years 1996 through 1998, OPM conducted, on yearly average, 4,276 SSBIs for Top Secret clearances. Of those, only 45.8 percent of the individuals investigated had no actionable issues, 35.2 percent had minor to moderate issues, and 6.3 percent of individuals investigated had substantial major issues of security concern in their background.[107] The record was even worse for the 18,477 Background and Limited Background investigations conducted annually. Of those, only 38.8 percent had no actionable issues, 43.1 percent had minor to moderate issues of concern, and 10.6 of the investigations raised substantial major issues of concern. Surprisingly, investigations for the lowest level clearances resulted in 61.7 percent of the applicants having no issues of concern and only 0.5 percent with major issues.

Periodic reinvestigations of previously cleared persons who currently held security clearances disclosed that a substantial number had issues of concern. Of the annual average of 23,334 such investigations, only 63.8 percent had no issues of concern, while 30.2 percent had from minor/moderate to substantial/major issues, including 2.4 percent in the worst category. The results of the periodic reinvestigations show a need for constant vigilance, as almost one-third of those reinvestigated showed issues of concern in their background investigation.

OPM Investigations

Currently, regulations pertaining to OPM's national security investigations are found at 5 C.F.R. Parts 732 and 736.[108] These regulations, in turn, refer to Chapter 732 of the *Federal Personnel Manual* (which was abolished in 1993) for the investigative requirements for each position sensitivity level.[109] The current regulations were adopted prior to the issuance of Executive Order 12968 and do not incorporate its new standards and procedures.

Proposed revisions to Parts 732 and 736 were published in January 1996 but as of January 1999 were still under consideration.[110] The proposed revisions incorporate the parts of the FPM, such as the investigative requirements and sensitivity levels of positions, included only by reference in the current regulations.

The granting of confidentiality to a source is far more restricted under the proposed regulations. Whereas now, there is no limitation on promising that a source's identity will be kept confidential, as proposed, a pledge of confidentiality could only be granted "in the most compelling circumstances and only upon specific request by the source." A pledge of confidentiality could not be assumed and, if granted, would extend only to the identity of the source or any information that might reveal the source's identity.[111]

OPM investigations are conducted in accordance with the OPM investigator's handbook, FPM Supplement 736-1, *Conducting and Reporting Personnel Investigations* (February 1999). In general, the criteria and standards in the handbook for each type of investigation are those described in the former Federal Personnel Manual. The handbook, however, is much more extensive than the FPM, covering in detail how an investigation is to be conducted, including how to distinguish truthful responses from deceit. It addresses the requirements for each type of investigation, how to conduct the field work portion of the investigation, how to conduct the personal interview of the subject of the investigation, and how to obtain information from record sources and from interviews with persons other than the individual being investigated. The handbook describes the process for evaluating and assigning seriousness codes to the information produced by the investigation.

The proposed regulations also incorporate the provisions regarding the use of the polygraph, formerly in the FPM.[112] Its use under either the former FPM or the proposed regulations is limited to those Executive Branch agencies which have a highly sensitive intelligence or counterintelligence mission directly affecting the national security, "e.g., a mission approaching the sensitivity of the CIA." All other Executive Branch departments and agencies are prohibited from initiating a polygraph examination for employment screening purposes for applicants or appointees to the competitive service.[113] Agencies desiring to use the polygraph for preemployment screening must obtain the prior approval of OPM and must adopt regulations in accordance with strict OPM standards specifying how the polygraph is to be used.[114] OPM does authorize the use of polygraphs during preemployment investigations of certain personnel in the Drug Enforcement Administration, including Special Agents and Intelligence Analysts. Some GSA employees assigned

to DoD communications and certain selected positions in the Secret Service and the Bureau of Alcohol, Tobacco, and Firearms are also polygraphed.

OPM allows its investigators to conduct only 10 percent of its investigations by telephone and continues to check on applicants' residences, finding that that produces substantial information.

CHAPTER 5

Adjudicative Guidelines for Determining Eligibility for Access to Classified Information

Development of the Guidelines

Before a prospective government employee, contractor employee, or member of the military can have access to national security information, that person must first undergo a background investigation. If anything questionable results, there will be an adjudication to determine whether the person is sufficiently trustworthy to hold a security clearance. The individual must meet certain criteria, known as the Adjudicative Guidelines, relating to their honesty, character, integrity, reliability, judgment, mental health, and association with undesirable persons or foreign nationals. In judging the person against the criteria, traits that might make the person susceptible to coercion, bribery or pressure, or cause him to act in a manner contrary to the best interest of the national security are examined. An employee or military member must continue to meet these criteria after being granted a clearance to remain eligible for access to classified information.

Although the United States Government has long had programs to protect national security secrets, it was not until 1953, with the issuance of Executive Order 10450, that the criteria for judging a person's eligibility for a security clearance were first formalized. That executive order remains in effect. The criteria formulated in Executive Order 10450, although often reworded and reworked, are essentially the same today as they have been for more than 45 years.

Because Executive Order 10450 is applicable to only government employees, Executive Order 10865 subsequently established guidelines for safeguarding classified information within industry. The later executive order did not establish separate suitability standards, so by directive of DoD the adjudicative criteria of the earlier executive order were made applicable to non-government employees.[115]

Over the years as administrations changed, each would issue its own executive order modifying and adjusting the systems, standards, and procedures for protecting national security information.[116] Also, each agency dealing with classified information applied its own interpretations to the standards for clearances of Executive Order 10450. Within DoD alone, interpretation and application of the standards fluctuated over time from very general to very specific to rather general again.

Because of inconsistencies among government agencies, resulting in agencies having to get multiple clearances for the same employee using different standards, legislation in 1994 required the Executive Branch "to establish uniform minimum requirements governing the scope and frequency of background investigations of all employees in the Executive Branch of government who require access to classified information as part of their official duties."[117] That requirement was binding on all departments,

agencies and offices of the Executive Branch for their employees, but did not apply to contractor employees.

The requirements of the statute were implemented by the issuance of Executive Order 12968 on August 2, 1995, which directed the Security Policy Board to develop a common set of adjudicative standards for background investigations for access to classified information.[118] It also extended the application of the law to the nongovernment workforce. Under the Executive Order, agencies were allowed to use any lawful investigative procedure to resolve issues that might arise during an investigation. The statutory mandate was further accomplished by the Security Policy Board's issuance of its Uniform Adjudicative Guidelines on March 24, 1997.[119]

Although not required by statute, the Executive Order and the Security Policy Board's Uniform Guidelines apply not only to all U. S. government civilian and military personnel, but also to consultants, contractors and their employees, and licensees and grantees of the government.[120] The Guidelines apply to collateral clearances, i.e., Confidential, Secret, and Top Secret, to determinations for access to Sensitive Compartmented Information and to Special Access Programs, and to "Q" and "L" accesses under the Atomic Energy Act.

The Security Policy Board also adopted Uniform Investigative Standards for all access investigations. Those standards allow for enhanced investigative requirements for certain Special Access Programs that may be specifically approved under Executive Order 12958.[121] The Uniform Standards require that investigations that meet the requirements at a given level must be mutually and reciprocally accepted by all agencies.[122]

The Uniform Adjudicative Guidelines

The Uniform Adjudicative Guidelines for determining access eligibility apply to all persons in the Executive Branch except the President and Vice President. They also apply to consultants, contractors and their employees, licensees, certificate holders and grantees and their employees, and to any other person acting for an agency who requires access to classified information, to Sensitive Compartmented Information, or to Special Access Programs. The application of the guidelines has been extended to the Judicial Branch, except for justices of the Supreme Court and judges who are exempt, by procedures established by the Chief Justice.[123] The guidelines apply not only to persons being considered for initial eligibility for access to classified information including applicants for employment, but also to those already having an access who have a continued need. Persons seeking or having access to Sensitive Compartmented Information and Special Access Programs are also judged by them. They are used by government departments and agencies in all final clearance determinations.[124]

The following "Uniform Guidelines," "Adjudicative Process," "Concerns," "General Considerations," "Disqualifying Conditions" and "Mitigating Conditions" are essentially as stated in the Adjudicative Guidelines issued by the Security Policy Board. The "Comments" following each guideline are those of the author.

The Uniform Guidelines

The guidelines for evaluating a person's eligibility for a clearance or access to classified information are the following:[125]

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

The Adjudicative Process

Determining a person's eligibility for access to classified information is more than just a mechanical application of the Adjudicative Guidelines. Eligibility is predicated not only upon an individual's meeting these personnel security guidelines, but on an examination of a sufficient period of a person's life to be able to make an affirmative determination that the person would not be a security risk. There must be a careful "common sense" weighing of a number of variables, known as the "whole person concept," in reaching a determination. This includes information both past and present, favorable and unfavorable about the person.

In evaluating the relevance of an individual's conduct, an adjudicator must consider the following factors:

(1) The nature, extent, and seriousness of the conduct;

(2) The circumstances surrounding the conduct, to include knowledgeable participation;

(3) The frequency and recency of the conduct;

(4) The individual's age and maturity at the time of the conduct;

(5) The voluntariness of the person's participation;

(6) The presence or absence of rehabilitation and other pertinent behavioral changes;

(7) The motivation for the conduct;

(8) The potential for pressure, coercion, exploitation, or duress; and

(9) The likelihood of a continuation or recurrence of the conduct.[126]

The Adjudicative Guidelines require that each case must be judged on its own merits, but that any doubt must be resolved against granting access to classified information. In the end, there must be a finding that it is clearly consistent with national security to grant an individual a clearance and access.

Although adverse information concerning a single guideline may be insufficient to require an unfavorable determination, an individual may be disqualified if information reflects a recent or recurring pattern of questionable judgment, irresponsibility or emotionally unstable behavior. Notwithstanding the "whole person" concept, an investigation may be terminated if significant, reliable, disqualifying, adverse information becomes apparent. The final determination remains the responsibility of the Department or agency having the classified information.[127]

When information of a security concern becomes known about an individual who currently holds an eligibility for access to classified information, the adjudicator must also consider whether the person:

(1) Voluntarily reported the information;

(2) Was truthful and complete in responding to questions;

(3) Sought assistance and followed professional guidance where appropriate;

(4) Resolved or appears likely to favorably resolve the security concern; and

(5) Has demonstrated positive changes in behavior and employment;

After evaluating the information of security concern, the adjudicator may consider temporarily suspending the person's access pending a final adjudication. Where the information is not serious enough to warrant a revocation of a security clearance, the clearance may be continued with a warning that future incidents of a similar nature may result in revocation of access.[128]

Comments[129]

The importance of the "whole person" concept cannot be over emphasized. Conduct by one person that is unacceptable might not disqualify another. For example, the use of a variety of drugs by a person in high school or college, even to a substantial degree, might not disqualify that person, while a single use of marijuana by an adult while that person held a security clearance would probably cause loss of a clearance. Also, a person active in his community and with a record of service to others would be more likely to retain his clearance after being caught shoplifting during a period of emotional stress, than someone with a series of minor traffic offenses and arrests for public disorder involving alcohol.[130] Someone with a diligent work record and a history of adherence to

rules and regulations would be more likely to retain his clearance after a single violation of security regulations than someone with the same violation who habitually disregarded work rules.

In an adjudication of an alleged violation of the guidelines, testimony or affidavits by a spouse, parent, clergy, physician, supervisor, coworker, or neighbor, as appropriate to the situation, can often provide information about the individual's "whole person" which would not be found in the investigative file of the alleged violation of the guidelines.[131]

Guideline A—Allegiance to the United States[132]

The Concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Disqualifying Conditions:

(1) Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

(2) Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(3) Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means; or

(4) Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Mitigating Conditions:

(1) The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(2) The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(3) Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest; or

(4) The person has had no recent involvement or association with such activities.

Comments

Guideline A is probably the least-used guideline for denying or revoking a clearance.[133] The Defense Security Service is required, if it discovers involvement with sabotage, espionage, treason, or efforts to overthrow the government by unconstitutional means, to turn the matter over to the appropriate counterintelligence agency or the FBI for investigation and ultimately criminal prosecution.[134] More problematic is a person's involvement with organizations whose aim is to prevent others from exercising their constitutional rights, such as the Ku Klux Klan or anti-abortion groups that engage in acts of physical violence. The line between opinion and action is often a fine one, and the guideline draws that line at "involvement in activities." No such line is drawn, however, when it comes to sabotage, espionage, or treason. In that case, "sympathy" with persons attempting to commit such acts is sufficient grounds to resolve "any doubt in favor of the national security."

An issue sometimes arises with organizations having both a violence-advocating arm and one that provides humanitarian relief. While involvement with only the humanitarian aspects of such an organization is not grounds for losing a clearance, the argument is made that contributions for such purpose permits the organization to divert funds, otherwise used for humanitarian relief, to acts of violence.

Guideline B—Foreign Influence[135]

The Concern. 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 not citizens of the United States or 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:

(1) An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

(2) Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

(3) Relatives, cohabitants, or associates who are connected with any foreign government;

(4) Failing to report, where required, associations with foreign nationals;

(5) Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

(6) Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

(7) Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure; or

(8) A substantial financial interest in a country, or in any foreign-owned or foreign-operated business that could make the individual vulnerable to foreign influence.

Mitigating Conditions:

(1) A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

(2) Contacts with foreign citizens are the result of official United States Government business;

(3) Contact and correspondence with foreign citizens are casual and infrequent;

(4) The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country; or

(5) Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

Comments

As with Guideline A, any concerns regarding contacts with foreign intelligence organizations or exploitations by foreign governments would be referred to a counterintelligence organization of the United States Government or the FBI for investigation and possible criminal prosecution. From a clearance standpoint, what is frequently at issue are first- or second- generation Americans who have family living with them who have not become naturalized, or who still have close relatives living in foreign countries. It is not the allegiance of the person with the clearance that is the concern, addressed in Guideline A, but the possibility that a foreign government would attempt to coerce that person by threatening the safety or welfare of the relatives living abroad. The closer the family tie, the greater the possibility of influence.[136]

Also of concern are the actions of a person traveling in a foreign country that might make them subject to coercion after returning home, such as an illicit sexual relationship or the use of drugs. Using agent provocateurs to secretly photograph otherwise well-intentioned persons in compromising situations for use in blackmail to acquire government secrets is not unknown to foreign governments.

Guideline C—Foreign Preference[137]

The Concern. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he may be prone to provide information or make decisions that are harmful to the interests of the United States.

Disqualifying Conditions:

(1) The exercise of dual citizenship;

(2) Possession and/or use of a foreign passport;

(3) Military service or a willingness to bear arms for a foreign country;

(4) Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

(5) Residence in a foreign country to meet citizenship requirements;

(6) Using foreign citizenship to protect financial or business interests in another country;

(7) Seeking or holding political office in the foreign country;

(8) Voting in foreign elections; or

(9) Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

Mitigating Conditions:

(1) Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(2) Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

(3) Activity is sanctioned by the United States; or

(4) The individual has expressed a willingness to renounce dual citizenship.

Comments

Becoming a naturalized United States citizen does not automatically end foreign citizenship, as many foreign countries permit dual citizenship. Also, some countries grant automatic citizenship to the offspring of their citizens regardless of where the children are born. It is the exercise of rights under a foreign citizenship or the acceptance of benefits from a foreign government because of that citizenship that is of concern.[138] Those acts are indicators of possible dual loyalty or possible coercion through the termination of foreign benefits. While renunciation of a foreign citizenship is not absolutely required, it is the clearest indicator of a single loyalty to the United States.[139]

Guidance D—Sexual Behavior[140]

The Concern. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, subjects the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

Disqualifying Conditions:

(1) Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(2) Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

(3) Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; or

(4) Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.[141]

Mitigating Conditions:

(1) The behavior occurred during or prior to adolescence, and there is no evidence of subsequent conduct of a similar nature;

(2) The behavior was not recent, and there is no evidence of subsequent conduct of a similar nature;

(3) There is no other evidence of questionable judgment, irresponsibility, or emotional instability; or

(4) The behavior no longer serves as a basis for coercion, exploitation, or duress.

Comments

Sexual behavior as a basis for denying or revoking a security clearance is fraught with the most uncertainty of any of the guidelines. Behavior that is legal in one state might be illegal in another, such as cohabitation by unmarried consenting adults. Adultery may be considered the exercise of poor judgment, but if the spouse forgives or accepts such behavior, it is questionable whether, in the mores of today's society, it should be a reason for denying a security clearance.[142] It is unquestionable, however, that this guideline prohibits clearly criminal behavior, such as pedophilia or incest.[143] In addressing these issues, the "whole person" concept and the "common sense determination" of the adjudicative authorities become most important.[144]

This guideline (and Executive Order 12968) specifically excludes sexual orientation or preference as a basis for denying a clearance.[145] However, if one's sexual orientation or preference is not openly acknowledged, that becomes a security concern because of the potential for coercion.[146] That concern for coercion is not limited to only homosexual activity but also to heterosexual activity such as adultery which might be cause for blackmail.

Whether to disclose a homosexual or lesbian relationship can be a Hobson's choice in relation to keeping a security clearance. Under the "Don't ask—Don't tell" policy of the military, disclosure of a homosexual or lesbian relationship, except in the context of a security clearance investigation, would lead to dismissal from military service, but failure to openly acknowledge such a relationship could result in the loss of a security clearance necessary for a military assignment.[147] Disclosure of some types of sexual conduct during the course of a security clearance investigation may be reported to the military service, which could lead to a criminal investigation or an administrative discharge. In the case of an officer, failure to disclose would cause the loss of a security clearance that surely would lead to dismissal from military service, as a clearance is a prerequisite to such service.

Guideline E—Personal Conduct[148]

The Concern. Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(1) Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

(2) Refusal to complete required security forms, releases, or provide full, frank and truthful answers to unlawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination:

Disqualifying Conditions:

(1) Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

(2) The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(3) Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other representative in connection with a personnel security or trustworthiness determination;

(4) Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duties, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

(5) A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency; or

(6) Association with persons involved in criminal activity.

Mitigating Conditions:

(1) The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

(2) The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

(3) The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

(4) Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

(5) The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

(6) A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security proc-

essing requirements, and, upon being made aware of the requirement, fully and truthfully provided the requested information; or

(7) Association with persons involved in criminal activities has ceased.

Comments

Guideline E is a catchall for any types of conduct not otherwise prescribed and is an overlap of all of the other guidelines. This guideline is a combination of former Criterion "I" which barred "acts of omission or commission that indicated poor judgment, unreliability, and untrustworthiness," and former Criterion "O" which barred "any knowing and willful falsification, cover-up, concealment, misrepresentation, or omission of a material fact" from any written or oral statement given to the government. Because a violation of any other guideline is also a violation of this one, it is the government's practice, when charging a violation of any of the other guidelines to generally also charge a violation of Guideline E.[149]

Failure to cooperate with a personnel security investigation is virtually an automatic disqualifier.[150] Also, providing false or misleading information during the investigation will most likely disqualify the Subject.[151] To overcome that disqualifier, the subject of the investigation must show that he misunderstood the request for information or had some reasonable explanation, such as embarrassment if his employer learned of the information, or that he wanted to make a full personal disclosure to the government investigator. Disclosures made during a polygraph after repeated evasions are not likely to overcome the disqualifier.

Any omitted facts must be material. For example, if in providing an employment history, a part-time job during high school was omitted, it would not be grounds for denying a clearance to a Ph.D. physicist, unless there was something at the job, such as criminal involvement, which the applicant sought to hide.

A frequent reason for denying of a clearance under this guideline is the failure to file federal and state income tax returns. Though no taxes may be owed, the failure to file is considered an unwillingness to follow rules and regulations and a violation of criminal law. Generally, if a person completes his filings by the time of the adjudication, a clearance will be granted. However, if there are subsequent failures to file, as often occurs, the clearance will generally be revoked.

This guideline permits an open-ended inquiry when disqualification can be based on "reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances." A disgruntled neighbor may report the unkempt state of the subject's front lawn or that his house was not regularly painted to neighborhood standards. Supervisors may report that the person did not take direction well or did not socialize with coworkers. Subjective reports such as these in the record of investigation have been used as a basis to charge that a person should not have a security clearance because of questionable judgment.

Guideline F—Financial Considerations[152]

The Concern. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Disqualifying Conditions:

(1) A history of not meeting financial obligations;

(2) Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statement, and other intentional financial breaches of trust;

(3) Inability or unwillingness to satisfy debts;

(4) Unexplained affluence; or

(5) Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Mitigating Conditions:

(1) The behavior was not recent;

(2) It was an isolated incident;

(3) The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, a death, divorce or separation);

(4) The person has received or is receiving counseling for the problem, and there are clear indications that the problem is being resolved or is under control;

(5) The affluence resulted from a legal source; or

(6) The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

Comments

History has shown that the need for money has often been the cause of traitors revealing national security information. Excessive debt is viewed as one of the most serious possible sources of coercion. As the guideline indicates, debt itself is not as critical as the reasons for one's being in debt and the efforts being taken to resolve it.[153] Filing for bankruptcy does not cause an automatic revocation of a clearance. If the bankruptcy resulted from a profligate use of credit for purchasing luxuries, it will be viewed as resulting from poor judgment and lack of concern for others.[154] If, on the other hand, it was

caused by factors beyond the debtor's control, such as unexpected medical bills, the filing may be viewed positively since excessive debt will have been eliminated as a possible source of coercion. Debt alone will not cause the revocation of a clearance if the person is making good-faith efforts to repay the debt within their means.[155]

Unexplained affluence as a basis for denying or revoking a clearance is, as has been previously, in the Adjudicative Criteria. Had it been applied in the case of former CIA employee, Aldrich Ames, who was able to buy, unnoticed, a $540,000 house for cash on a mid-level government salary, some of his espionage might have been prevented. Statutes and regulations requiring financial disclosure as a condition for a security clearance enacted since his exposure should prevent a reoccurrence.

Guideline G—Alcohol Consumption[156]

The Concern. Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses and increases the risk of unauthorized disclosure of classified information due to carelessness.

Disqualifying Conditions:

(1) Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

(2) Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition or drinking on the job;

(3) Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(4) Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker, who is a staff member of a recognized alcohol treatment program;

(5) Habitual or binge-consumption of alcohol to the point of impaired judgment; or

(6) Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

Mitigating Conditions:

(1) The alcohol-related incidents do not indicate a pattern;

(2) The problem occurred a number of years ago, and there is no indication of a recent problem;

(3) Positive changes in behavior supportive of sobriety; or

(4) Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

Comments

Alcohol, drug abuse and financial instability are the three most common reasons for denial or loss of a security clearance.[157] The government need not show that the individual is an alcoholic, an alcohol abuser, or alcohol dependent. Several incidents of alcohol-related incidents at or away from work are sufficient to question a person's judgment or reliability.[158] The more serious the incident the fewer incidents will be required to revoke a clearance. Even if there have been no incidents, excessive consumption alone can be the basis for denial or loss of a clearance.

The disqualifying conditions of this guideline are the easiest in theory and the hardest in practice to overcome. Ideally, if a person enters and successfully completes an alcohol rehabilitation program, and abstains from alcohol for at least 12 months, the clearance should be restored. Accomplishing that, however, is sometimes extremely difficult. Despite the minimum of a year's abstinence as stated in the guideline, adjudicative authorities generally look for at least two to three years before they will restore a clearance.[159]

Guideline H—Drug Involvement[160]

The Concern. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

Drugs are defined as mood- and behavior-altering substances, and include (a) drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and (b) inhalants and other similar substances. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Disqualifying Conditions:

(1) Any drug abuse;

(2) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

(3) Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(4) Evaluation of drug abuse or drug dependence by a licensed clinical social worker, who is a staff member of a recognized drug treatment program; or

(5) Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

Mitigating Conditions:

(1) The drug involvement was not recent;

(2) The drug involvement was an isolated or aberration event;

(3) A demonstrated intent not to abuse any drugs in the future; or

(4) Satisfactory completion of a prescribed drug treatment program including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

Comments

Drug involvement is a security concern because of the possible impairment of judgment and because of its indicativeness of a person's selective adherence to the law. While some would argue that smoking a marijuana cigarette to relax on the weekend is no more impairing than drinking a beer, the fact remains that marijuana is illegal and alcohol is not.

Any illegal drug use, possession, purchase, sale, or distribution is grounds for denial or revocation of a clearance. While the former Adjudicative Criteria were very specific in listing the recency of use and the amount and type of illegal substance used as factors to be considered in mitigation, the current guideline simply requires that it was "not recent," and "an isolated or aberration event."[161] Wide latitude is left to the adjudicative body to consider mitigating facts, and there is no assurance of consistency from board to board or case to case.[162]

Finding anyone graduating from college today who has not used illegal substances at some time is difficult. If the test were that only a person who never used or abused drugs could get a clearance, there would probably be few people in government or the defense industry under the age of 60. For that reason, much latitude is given to substance abuse in high school and college.[163] Once a person has graduated, however, the assumption is that he has entered the working world and matured.[164] Much less leeway is given after that time.

When prior substance abuse is self-reported in a personnel security questionnaire, the individual will be asked during a personal interview whether he intends to refrain from the use of any illegal substances in the future. Unless an unqualified "yes" is given, he will be denied a clearance.

No leeway will be given to any drug abuse while one holds a clearance.[165] The government adheres to a zero-tolerance drug policy. Drug abuse after a clearance is granted is considered a willful breach of security regulations and will be grounds for revocation of the clearance and loss of a job, if it is a job for which a clearance is necessary.[166]

Guideline I—Emotional, Mental, and Personality Disorders[167]

The Concern. Emotional, mental and personality disorders 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. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to, or approved by, the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and, particularly, for consultation with the individual's mental health care provider.

Disqualifying Conditions:

(1) An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

(2) Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

(3) A pattern of high-risk, irresponsible, aggressive, antisocial, or emotionally unstable behavior; or

(4) Information that suggests that the individual's current behavior indicates a defect in his judgment or reliability.

Mitigating Conditions:

(1) There is no indication of a current problem;

(2) Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control, or in remission, and has a low probability of recurrence or exacerbation;

(3) The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

Comments

In the past, individuals holding positions requiring access to classified information were often afraid to get or to report any type of psychological counseling for fear that any contact with a mental health counselor would result in the loss of a clearance. Executive Order 12968 specifically addressed that concern stating: "No negative inference... may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations."[168] If mental health counseling is indicated, the executive order allows further inquiry to determine if the Adjudicative Guidelines have been satisfied.

The guideline recognizes that mental health counseling may be necessary and temporary at times of personal stress, such as a death in the family, illness, or marital problems. It further recognizes that many mental health problems that in the past were intractable are now curable or can be controlled by medication. Nevertheless, serious mental disorders that do not respond to medical treatment will bar an individual from access to classified information.

Behavior that does not rise to the level of a serious mental disorder can still result in the loss of a clearance, and it is this category that is the most problematic. Included among this concern are "personality disorders" that can cause "a significant deficit in an individual's social and occupational functioning." The disqualifying conditions may be "a pattern of high-risk, irresponsible, aggressive, antisocial, or emotionally unstable behavior." Assessment of behavior in this category is the most subjective and may depend as much on the personality of the investigator as on the applicant for a clearance. Under the guideline, theoretically an engineer who liked to race motorcycles on the weekend might be considered to exhibit "high-risk, irresponsible" behavior, or a physicist who was unconcerned about his clothing fashion might be viewed as showing a deficit in social functioning, or a computer programmer who did not socialize with his coworkers might be considered to have a deficit in his occupational functioning. In general, however, only if a credible credentialed mental health professional were to say that the personality characteristics affected the person's judgment and reliability in ways that made him untrustworthy would the clearance be denied or revoked. This is a difficult of line to draw, and one that could eliminate the most brilliant from working on the national defense, if judged by their eccentric and nonstandard habits. A common sense approach becomes most important in separating behavior that simply varies from social standards to that which is an identifiable mental health condition.

Guideline J—Criminal Conduct[169]

The Concern. A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Disqualifying Conditions:

(1) Allegations or admissions of criminal conduct, regardless of whether the person was formally charged; or

(2) A single serious crime or multiple lesser offenses.

Mitigating Conditions:

(1) The criminal behavior was not recent;

(2) The crime was an isolated incident;

(3) The person was pressured or coerced into committing the act, and those pressures are no longer present in that person's life;

(4) The person did not voluntarily commit the act, and/or the factors leading to the violation are not likely to recur;

(5) Acquittal; or

(6) There is clear evidence of successful rehabilitation.

Comments

Conviction of a serious crime will certainly cause the denial or revocation of a security clearance.[170] What becomes questionable is when there has been no conviction.[171] Often, criminal charges will not be reported by the individual involved because the charge has been dismissed, or the conviction was later expunged. The charge may be later discovered as part of a personnel clearance investigation of local criminal records or FBI indexes, thus creating further problems for the subject in explaining why their response to the Security Questionnaire was incomplete.

For the purposes of a security clearance, it is not the outcome of the charge that is important, but the nature and gravity of the underlying conduct and the reason for the dismissal or expungement of the charge.[172] If a dismissal is for technical reasons, such as untimeliness in bringing the charge or as a result of a policy of leniency for first offenders, the underlying charges will be considered as part of the security review.[173] If the dismissal or acquittal was because there was no factual basis to the charge, that, too, will be considered.

Multiple, less serious offenses, or offenses that might be considered "administrative," may also be reason for denying or revoking a clearance. Among these is failure to file state or Federal income tax returns.[174] Though no taxes may have been owed, and the taxing authorities imposed only civil penalties, because there are statutes that do provide for criminal penalties, a violation on this basis may be sustained. A series of minor traffic offenses, each of which individually would not be considered sufficient, in the aggregate

might also be considered a violation of this guideline as evidencing at least a disregard of societal rules.

Guideline K—Security Violations[175]

The Concern. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Disqualifying Conditions:

(1) Unauthorized disclosure of classified information; or

(2) Violations that are deliberate or multiple or due to negligence.

Mitigating Conditions:

Actions that:

(1) Were inadvertent;

(2) Were isolated or infrequent;

(3) Were due to improper or inadequate training; or

(4) Demonstrate a positive attitude towards the discharge of security responsibilities.

Comments

Failure to comply with security regulations is viewed as among the most serious of violations of the guidelines, as it goes to the very heart of the security process.[176] Willful disclosure of classified information will certainly lead to the revocation of a clearance and may result in criminal prosecution, even if not done with subversive intent.[177] Repeated unintentional infractions, even if minor, may also lead to the revocation of a clearance.[178] Examples are inadvertently shredding a classified document without properly accounting for it or leaving a computer disc in a desk drawer at the end of the day, rather than locking it in an authorized safe.[179] Such conduct is considered indicative of a lack of the diligence required for the protection of classified information. While a first or second violation may result in a reprimand, subsequent infractions of security regulations, even if unintentional and not causing a compromise of classified information, will likely lead to the revocation of a clearance.

Guideline L—Outside Activities[180]

The Concern. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security

responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Disqualifying Conditions:

Any service, whether compensated, volunteered or employed, with:

(1) A foreign country;

(2) A foreign national;

(3) A representative of any foreign interest; or

(4) A foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Mitigating Conditions:

(1) Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities; or

(2) The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his security responsibilities.

Comments

Activities most likely to cause concern under this guideline are memberships in scientific and technical professional organizations.[181] Such organizations frequently publish research that, although not classified, may relate to the classified work being done by the cleared individual. Of concern is the possibility of disclosure, at meetings or symposia, of unclassified information gained through classified research, being combined with other unclassified information to give insight into classified work. Obtaining prior authorization by the cleared individual to attend meetings or to make such presentations is probably the safest way to avoid the possibility of a violation of this guideline.

Guideline M—Misuse of Information Technology Systems[182]

The Concern. Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information technology systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Disqualifying Conditions:

(1) Illegal or unauthorized entry into any information technology system;

(2) Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system; or

(3) Removal or use of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations.

Mitigating Conditions:

(1) The misuse was not recent or significant;

(2) The conduct was unintentional or inadvertent;

(3) The introduction or removal of media was authorized;

(4) The misuse was an isolated event; or

(5) The misuse was followed by a prompt, good-faith effort to correct the situation.

Comments

Although it would appear that the information technology systems to which this guideline refers are those used for classified or sensitive systems, in the several reported cases from DOHA and DOE it has been applied to nonclassified and nongovernment computers and to commercial copyrighted software.[183] The use of a nonclassified government computer for viewing "adult" material on the Internet has been the basis for denying a security clearance.[184] Like the other guidelines, willful and criminal violations of this guideline will assuredly cause loss of a clearance. The unintentional or noncriminal violations are more frequently the subject of a security investigation.

The occasional use of a personal computer for preparing a shopping list or a personal letter, while an unauthorized use of government property, is far from a rarity. The use of Tempest-shielded computers for such a purpose, however, puts the use on an information technology system that the guideline specifically addresses. Although the preparation of a personal letter or shopping list is a violation of the guideline, it is the more serious misuse of equipment used to process, manipulate, or store classified or sensitive data that is of greater concern. Taking home a computer disc containing classified information to work on it, though well-intentioned, is a prohibited violation. Failing to remove and secure a hard drive containing classified information at the end of the workday is another violation. It is such actions, although well-intentioned or inadvertent, that are a cause of security concern.

CHAPTER 6

Military and Defense Civilian Employee Appeals of Adverse Clearance Determinations

Basis of Authority for Program

The Supreme Court in *Department of the Navy v. Egan* has held that "no one has a right to a security clearance" and that "the grant of a clearance is an affirmative act of discretion... only when clearly consistent with the interests of the national security."[185] That decision reflects what has been the policy and practice of the Executive Branch of the government since at least the modern origin of the government's program. It was first formalized in Executive Order 10450 in 1953. That Executive Order, still in effect, deals only with security requirements for civilian government employees. Similar standards and criteria have also been applied by Defense Department regulations to applicants for government employment, to military personnel, and to contractor employees under the Industrial Security Program. The present system for determining who will have access to classified information, how those determinations are made, and how decisions may be appealed was formulated in Executive Order 12968, signed by President Clinton in 1995. For Department of Defense civilian employees and military personnel, this system is implemented by DoD Directive 5200.2 and its corollary regulation, DoD 5200.2-R. Each of the military departments has its own regulation.[186]

Prior to the issuance of Executive Order 12968, DoD Regulation 5200.2-R provided that when a person's clearance was denied or revoked, he would be given: (a) a detailed statement of why the unfavorable action was being taken, (b) the opportunity to reply in writing to the authority that issued the statement of reasons, (c) a written response to the reply stating the final reason for the decision to deny or revoke a clearance, and (d) the right to appeal in writing to a higher authority in the DoD component concerned. There was no right to a personal appearance, no right to see or challenge the evidence on which the decision was based, no right to know or cross-examine the accuser, and no right to present testimony, either personally or by witnesses, to counter the accusations or to support the continuation of a clearance. This was the system approved by the Supreme Court in the *Egan* case. The Court never addressed the issue of due process because, it held, that there was "no right" to a security clearance, and without an enforceable right, there is no particular process due.[187]

The current standards embodied in Executive Order 12968 resulted from more than 11 years of discussion by two administrations.[188] In March 1983, President Reagan signed National Security Decision Directive 84 that directed, among other things, that a study group be formed to review the federal personnel security system and recommend revisions to existing Executive Orders and regulations. The study resulted in a report to the Secretary of Defense known colloquially as the Stilwell Commission report, recommending various changes.[189] A draft executive order was circulated to various agencies in January 1989 that would have authorized significant cutbacks in the procedural rights then afforded government employees and applicants. Opposition from members of

Congress, federal employee unions, the American Bar Association, and other groups caused the Executive Branch to reconsider and finally withdraw the proposal. With the change in administrations in 1992, a new study was undertaken which led to the amendment of the National Security Act of 1947, requiring uniform adjudication standards and procedures.[190] In 1995, Executive Order 12968 was adopted to carry out the requirements of the new law.

The new executive order did not provide to government employees all of the procedural safeguards already afforded to contractor employees, notably the right to a hearing. It did, however, for the first time provide government employees and applicants for employment the opportunity to present their side of the case and to have it heard outside the security establishment. Executive Order 12968, while not fully satisfying either those advocating a full due-process hearing or the security offices' desire for a quick and economical decision, balanced the need to protect the nation's secrets with an individual's right not to be unfairly deprived of his employment or professional career.

Rights and Procedures Under Executive Order 12968

E.O. 12968 makes a number of significant changes in the way security clearances are considered and granted or denied. For the first time, it imposes uniform standards on government agencies in granting security clearances and access to classified information. It directs the Security Policy Board to issue implementing standards within 180 days.[191] The executive order also makes the uniform standards applicable to applicants for government employment, members of the Armed Forces, and civilian government employees (as well as contractor employees). It prohibits discrimination based on race, sex, color, religion, national origin, disability, or sexual preference in the granting of access to classified information.[192]

Specific procedures for reviewing unfavorable access determinations are also provided by the executive order.[193] It provides that if an applicant or employee is determined not to have met the standards for access to classified information, the person will be: (a) given a written explanation for that conclusion, as detailed and comprehensive as permitted by the national security; (b) provided within 30 days, upon request, any documents, records, or reports upon which the denial or revocation was based, to the extent such documents would be available under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (5 U.S.C. 552a); (c) informed of their right to counsel at their own expense; (d) informed of the right to request the entire investigative file to the extent permitted by national security or other law, which if requested, must be provided prior to the time allowed for a written reply; (e) provided a reasonable time to reply in writing and to request a review of the determination; (f) provided with written notice of and the reasons for the results of the review and the identity of the deciding official and the right to appeal the review; (g) provided an opportunity to appeal in writing to a "high level panel" appointed by the agency head, comprised of at least three members, two of whom are outside the security field; and (h) provided the opportunity to appear personally and to present relevant documents, materials, or other information "at some point in the process" before an adjudicative or other authority, other than the investigative authority, which can be before the appeal panel itself. If the personal appearance of the individual is before

anyone other than the appeal panel, a summary or recording must be made to become part of the individual's security record. The decision of the appeal panel will be in writing and final unless the agency head personally exercises the appeal authority based on the recommendations of the appeal panel.

Although an applicant or employee now has the right to a personal appearance, that is not the same trial-type hearing afforded to contractor employees. There is no right to hear the live testimony of the government's witness or to cross-examine those witnesses, no right to present witnesses to testify on behalf of the employee or applicant, no right to see classified information that may be the basis of the denial, and no right to know of the identities of persons who may have given information with the promise of confidentiality. Where there is a personal appearance before a hearing officer or adjudicative authority other than the appeal panel, the finding and conclusions are not binding but are only recommendatory to the appeal panel. There does not have to be any record of evidence or testimony kept if the personal appearance is before the appeal panel itself.

The executive order provides the right to a personal appearance by the applicant or employee, with counsel, to testify and to present written evidence before a fact-finding body and the right to a decision by a panel composed of a majority of members outside the security field.

Appeals of SAP and SCI Access Decisions

Appeals of denials of access to Special Access Programs (SAPs) for government employees or military personnel are not required by Executive Order 12968, which leaves it to each agency that creates the SAP to establish procedures dealing with them.[194] To the extent possible and consistent with the national security, the executive order directs that the agency procedures be consistent with the standards and procedures of the order.[195] Most often, however, the person will never know that he has even been considered for access and rejected. The lack of any "due process" procedures in the SAP arena for government employees, like that of contractor employees, comes from the Supreme Court's decision in *Green v. McElroy,* which suggested that the President might have inherent authority to deprive a person of his employment in these special situations so long as it was done explicitly.[196] The Supreme Court's suggestion was adopted for government employees of the Executive Branch and military personnel by Section 2.2(b) of Executive Order 12968, and by DoD Regulation 5200.2-4, paragraphs 7-102 and 8-200. The exclusion of appeals of SAP access decisions by contractor employees is provided under Executive Order 10865. (See Chapter 7.)

Denials of access to Sensitive Compartmented Information to government employees are appealable under procedures established in Director of Central Intelligence (DCID 6/4) (See Chapter 10.)

Security Standards and Procedures Under DoD 5200.2-R

The vast majority of individuals employed by the government who are required to have national security clearances are civilian employees of the Department of Defense

and members of the armed forces. Their clearances are controlled by Department of Defense Personnel Security Program Regulation, DoD 5200.2-R.[197] Chapters 6, 7 and 8 of that regulation address adjudications, the issuance of clearances, and accesses and appeals of unfavorable clearance and access decisions.

Before a clearance or access is granted, the standard that must be met is that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the national security. That decision must be reached by using an overall common sense evaluation of all relevant information, both favorable and unfavorable, including prior experience in similar cases.[198] To ensure uniformity, the military departments and some other DoD components are required to establish a Central Adjudication Facility (CAF), to make personnel security determinations, and a Personnel Security Appeals Board (PSAB) to hear appeals of those determinations. Any proposed unfavorable determination must be signed by a civilian, of at least grade GS-11 or 12 or a military officer of rank O-4.[199]

Each of the military departments has supplementing regulations establishing its Central Adjudication Facility and Personnel Security Appeals Board.[200]

The relevant factors that must be considered for government employees and applicants are the same as those for contractor employees. They are: (a) the nature and seriousness of the conduct, (b) the circumstances surrounding the conduct, (c) the frequency and recency of the conduct, (d) the age of the individual, (e) the voluntariness of participation, and (f) the absence or presence of rehabilitation.[201]

Detailed adjudication guidelines are found in Appendix I to the DoD Regulation. This appendix was developed from the criteria first formulated in 1953 in Executive Order 10450, i.e., (a) allegiance to the United States; (b) foreign influence; (c) foreign preference; (d) sexual behavior; (e) personal conduct; (f) financial considerations; (g) alcohol consumption; (h) drug involvement; (i) emotional, mental, and personality disorders; (j) criminal conduct; (k) security violations; and (l) outside activities. These guidelines match the Uniform Adjudicative Guidelines approved by the White House on March 24, 1997. The DoD Guidelines include an additional category "M," of misuse of information technology systems.

The DoD regulation refers to DCID 6/4 for the adjudication policy for access to SCI.[202]

Appeals of Unfavorable DoD Determinations

Under DoD Regulation 5200.2-R, an interim suspension of a security clearance may be imposed by the commander or head of an organization, "if information exists which raises serious questions" about a person's ability or intent to protect classified information. No fixed time is mandated to end a suspension, but the regulation requires that suspensions exceeding 180 days must be closely monitored and managed until finally resolved.[203] There is also no appeal of a suspension. However, during a suspension the

employee is kept on the payroll and assigned duties that do not require access to classified information.

No final unfavorable personnel security clearance determination or access determination (except access to SAPs) may be made regarding a member of the armed forces, a civilian employee or a consultant of the DoD, or any person affiliated with the DoD without affording that person the appeal rights provided in DoD 5200.2-R. The person must be provided with a written statement of reasons (SOR) setting forth why the unfavorable administrative action is being taken. Upon request, the individual must be provided with copies of all releasable records or advised where to write to obtain such records.[204]

The individual may respond in writing to the appropriate CAF within 30 days from receipt of the SOR. The time for response is quite limited. The individual must give notice of his intent to respond within 10 days after receipt of the SOR, and must file a written response within 30 days. Any extension for more than 30 days must be by written request to the employing organization. Requests can only be granted by the CAF.[205] Failure to submit a timely response will result in forfeiture of all further appeal rights.

If the individual's response is not persuasive, the CAF will issue a Letter of Denial stating the final reasons for taking the unfavorable action as specifically as privacy and national security considerations permit. Denial of a clearance or access may be expected between 60 and 90 days after the CAF's response. Following the CAF's denial, the person may appeal without a personal appearance directly to the component's Personnel Security Appeals Board (PSAB) or may have a personal appearance by requesting one before the Defense Office of Hearings and Appeals (DOHA). The personal appearance will be heard by an administrative judge of DOHA, the same judges who also conduct full administrative hearings on the record for defense contractor employees.

DOHA will schedule a personal appearance and will provide its "recommendations" to the appropriate PSAB, generally within 60 days following receipt of the request for the personal appearance.[206] The findings and conclusions of the DOHA administrative judge are recommendations only, which the PSAB may accept, reject, or modify as it sees fit. Following receipt of the appeal, or if there is a personal appearance, receipt of the recommendations of the DOHA administrative judge, the PSAB will provide a written decision including its rationale for the decision, normally within 30 to 60 days. The decision of the PSAB is final and not appealable.[207]

Personnel Security Appeals Boards consist of three members of at least military grade O-5 or civilian grade GM/GS-14. At least one member of the board must be equal or senior in grade to the appellant.[208] Although the regulation requires that one member of the board be a permanent member, and have knowledge and experience in the field of personnel security to provide consistency in decisions, in practice, the "permanent member" is sometimes a military officer assigned for a short period and then replaced, so there is no real institutional memory and often no consistency in decisions. One of the three board members must be an attorney unless the board has access to legal counsel, and not

more than one member may be from the security career field. Officials of the CAF may not serve on a PSAB or communicate with it on the merits of any open case. The PSAB's decision, either sustaining or overturning the original CAF determination, is final and concludes the process.

Personal Appearances Before DOHA

If an individual requests a personal appearance, the matter will be referred to DOHA which will assign the case to an administrative judge, who will schedule the personal appearance, generally within 30 days from the date of the request.[209] The personal appearance will be scheduled at the individual's duty station, or close to it if within the lower 48 states. If not, the hearing may be scheduled at the person's place of employment or at DOHA's offices in Arlington, VA, or the Los Angeles, CA, area.

The regulations establishing the procedures for the conduct of the personal appearances are very perfunctory. They simply require that the administrative judge conduct the proceeding "in a fair and orderly manner." The appellant may be represented by legal counsel or by a non-lawyer personal representative. Approximately three percent of individuals seeking a personal appearance before DOHA are represented by counsel.[210] The individual, either personally or through counsel, may make an oral presentation and may respond to questions by his counsel, his personal representative or by the administrative judge. No DoD department or agency currently provides legal counsel for its civilian employees, but the Navy, unlike the other military departments, does provide legal counsel for its military personnel.

The appellant may submit documents relevant to whether the adverse determination should be overturned but may not present witnesses. Because the government's witnesses will not be present, the appellant will have no opportunity to cross-examine them.

On completion of the proceeding, the administrative judge will provide a written recommendation to the PSAB along with any documents submitted by the appellant. The regulations do not make the administrative judge's recommendation either presumptively correct or binding, so the PSAB can accept, reject, or modify it at as it chooses.

Although DOHA's administrative judges apply the same standards to all cases referred to them, the outcome appears to depend on which military department referred the case. From December 1995, the beginning of the program, to April 1997, 514 cases have been referred for a personal appearance. Of those cases, DOHA has recommended reversing 32 percent of the initial CAF decisions and affirming 63 percent.[211] In those cases in which DOHA recommended affirmance of the initial CAF decision, the PSABs accepted its recommendation 96 percent of the time and reversed it in only 4 percent. Overall, the department's PSAB's accepted only 48 percent of DOHA's recommendations to reverse the initial CAF decision, choosing to accept the remainder of the CAF decisions.

A breakdown of these statistics by military departments shows an uneven treatment of DOHA's recommendations. The Army PSAB agreed with DOHA in 59 percent

of its recommendations to reverse the initial CAF decision, while the Air Force agreed with only 39 percent of DOHA's recommendations. Overall, of the first 326 personal appearance cases that have reached a conclusion, 78 percent have resulted in the affirmance of the initial CAF decision to withdraw or deny the clearance or access.

Timeliness is another area where actuality does not meet expectation. According to DoD 5200.2-R, DOHA is to provide a recommendation to the PSAB within 60 days after its receipt of a request for a personal appearance, and the PSABs are to issue a final decision within 30 to 60 days after receipt of the recommendation.[212] DOHA is thus doing better than the expected standard, averaging 49 days from receipt of notice of intent to appeal to decision. The PSABs do less well, averaging 87 days from their receipt of DOHA's recommended decision to their own final decision.[213] While that is the average, many final decisions take from 130 to 170 days.

Although the DoD regulation requires that the PSABs provide the reasons for their decision, whether it be sustaining or overturning the original CAF decision, for the most part they do not.[214] Generally, the final PSAB decision will simply be a statement affirming or reversing the CAF decision with no reason given and no explanation as to why a contrary DOHA recommended decision was rejected.[215]

DOHA does not provide a copy of its recommended decision to the employee or applicant before submitting it to the PSAB so there is no opportunity for that person to file objections or to note any errors. The PSABs also generally do not provide the employee with a copy of DOHA's recommended decision with their final decision since it is not required by regulation. DOHA does, however, automatically send a copy of its recommended decision to the employee or applicant after the final PSAB decision is issued.

CHAPTER 7

Contractor Employee Appeals of Adverse Clearance Determinations

Basis of Authority for Program

The right of employees of government contractors to appeal adverse security clearance determinations stems from the 1951 Supreme Court Decision, *Green v. McElroy.* That case held that absent a clear statement by Congress or the President declaring that such procedures are not needed, an individual is entitled to a full hearing to confront his accusers when faced with the loss of a security clearance that would deprive him of his right to follow his chosen profession.[216] To implement the court's ruling, President Eisenhower in 1960 issued Executive Order 10865, which was further carried out by Department of Defense Directive 5220.6. Both the 1960 Executive Order and the DoD Directive, as amended, remain in effect to this day.

The provisions of DoD Dir. 5220.6 have, by mutual agreement, been extended to 20 other federal departments and agencies.[217] Absent, however, are the Central Intelligence Agency, the National Reconnaissance Organization, the Federal Bureau of Investigation and the Department of Energy, all of which have their own contractor review procedures. Since the DoD Directive by its terms excludes cases dealing with access to Sensitive Compartment Information (SCI) and access to Special Access Programs (SAPs), the lack of inclusion of the CIA and NRO from its coverage has no real effect on contractors with those agencies, as everything they do falls within one or both of those categories.[218] The Department of Energy, having jurisdiction under the Atomic Energy Act, conducts its own security review program that offers procedural protections similar to those in the DoD Directive. DOE's program is discussed in Chapter 13. Procedures for appealing decisions denying access to SCI under Director of Central Intelligence Directive 6/4 (DCID 6/4) are discussed in Chapter 10.

There are no formal procedures for protesting a denial of access to a SAP. Generally, the person whose access is denied will never know that he or she has even been considered and rejected. This lack of any "due process" procedures in the SAP arena also arises from *Green v. McElroy,* which suggested that the President might have inherent authority to deprive a person of his employment in these situations so long as it was done explicitly.[219] The Supreme Court's suggestion, as it applied to contractor employees, was adopted by the Executive Branch in Executive Order 10865, § 9, and DoD Directive 5220.6, Paragraph B.6. Government employees are also explicitly excluded from appealing SAP access decisions by Executive Order 12968.

The Preliminary Determination to Deny a Clearance

On completion of a security clearance investigation by the Defense Security Service (DSS), the investigative file is referred to a branch of that agency, the Defense Industrial Security Clearance Office (DISCO) in Columbus, OH, for review. If no, or minimal, questionable information is found, the person is granted a clearance. However,

if sufficient derogatory information exists to question a person's suitability to hold a clearance, the case is referred to the Defense Office of Hearings and Appeals (DOHA) for further adjudication.[220] If the potentially disqualifying information precludes DOHA security specialists from concluding that it is clearly consonant with the national interest to grant a security clearance, a Statement of Reasons (SOR), analogous to a civil complaint or a criminal indictment will be prepared, stating in some detail the factual and legal bases for proposing to deny the clearance. The legal bases are couched in terms of the Uniform Adjudicative Guidelines issued by the Security Policy Board (as further discussed in Chapter 5).[221] The person seeking the clearance, i.e., the applicant, is sent the SOR and given 20 days to file a written answer under oath, either admitting or denying the charges. He may elect to have a hearing before an administrative judge or to have the case decided on the written record. The procedures at DOHA are specified in DoD Dir. 5220.6 and its three enclosures, which are sent to the applicant along with the SOR.[222]

Procedures at DOHA

The SOR consists of a series of numbered paragraphs, each a mixture of factual allegations and legal conclusions.[223] The factual allegations often cover numerous events over a long period. The conclusions of law charge that the alleged facts violate one or more of the Adjudicative Guidelines or federal statutes and regulations. Based on those charging paragraphs, the SOR will conclude that the applicant is unsuitable to hold a clearance because it is not in the national interest.[224]

DOHA requires that the applicant submit a "detailed written answer to the SOR under oath." A general denial of the charges is insufficient. Because the SOR often mixes factual allegations and legal conclusions, unless an applicant intends to admit that he is unworthy of holding a security clearance, he must deny each paragraph individually and admit only those particular facts he does not intend to contest. An applicant may choose to not contest some or all of the factual allegations, but defenses and mitigating circumstances may exist which, if raised, would avoid a finding of unsuitability. If an applicant files an answer admitting to the entire SOR, including the legal conclusions, and then on reflection or after retaining counsel amends his answer admitting only to those facts that are truly uncontested, both the first and second answers may be considered by the administrative judge in reaching a determination.[225]

An applicant, in answering the SOR, may request a hearing before an administrative judge. If that right is waived, or if a hearing is not requested with the answer, the case will be decided by an administrative judge based on the written record. DOHA is fairly liberal in allowing late requests for hearings, particularly when an applicant, who initially answers *pro se,* waives a hearing, but later retains counsel who requests it.

Hearings are normally held within a metropolitan area near the applicant's place of employment or residence. Since the administrative judges and the government's attorneys, referred to as "Department Counsel," are based at one of the three DOHA offices in Arlington, VA, Van Nuys, CA, or Boston, MA, they are fairly flexible in determining the location of a hearing. A hearing may be in a Federal office building or a local or federal

courthouse at a place selected for the convenience of the applicant, witnesses for both sides and counsel.

DOHA procedures provide for "at least 15 days notice of the hearing date," but that, too, is reasonably flexible to allow for the convenience of the appellant, appellant's counsel, Department Counsel, the availability of witnesses, and the administrative judge's schedule.

Discovery

Discovery is quite limited. The DOHA Procedural Guidance requires that where an administrative hearing is not requested, Department Counsel shall give the applicant "all relevant and material information that could be adduced at a hearing."[226] In practice, Department Counsel provides only those documents that it intends to introduce as evidence in its case and does not provide any exculpatory or favorable character evidence that could be used by the applicant in presenting his case. Department Counsel always has the complete DSS investigative file that invariably contains some favorable information, but will not provide that file unless a specific discovery request is made for it. Often a request is made too late for effective use to be made of the file. The DSS investigative file is available to the applicant at any time after the conclusion of the investigation by making a written request to the DSS Baltimore, MD, office under the Privacy Act. If a DOHA hearing has been scheduled and that is noted in the request, DSS will expedite providing the file.

DOHA procedures limit discovery by the applicant to "non-privileged documents and materials subject to control by DOHA."[227] Normally, documents in the possession of a "client" are not protected from discovery simply because they have not been turned over to their attorney. This is not true at DOHA. Department Counsels, who are employees of DOHA, take the position that although they are representing the interests of an agency in the Department of Defense or some other agency which may grant the security clearance, unless the documents are actually in DOHA's possession, they are not "subject to its control" and are, therefore, protected from discovery. This results in documents which are held by DSS or one of the agencies administering the applicant's classified contract being protected from discovery. If DSS omits or "redacts" a part of the investigative file before delivering it to DOHA, Department Counsel's position is that the applicant must file a Freedom of Information Act or Privacy Act appeal with DSS to get the remainder of the file. As a practical matter, that would result in years of litigation in the federal courts, making that avenue of discovery quite illusory in DOHA proceedings. Thus far, Department Counsel's position has been sustained by the administrative judges.[228]

Discovery requests by Department Counsel for information from the applicant is discretionary with the administrative judge and may be granted only on a showing of good cause.[229]

DOHA's procedures require that "as far in advance as practical," Department Counsel and the applicant exchange proposed documentary evidence.[230] Since the

procedures do not specify any time limits, the government's documents are often not provided until very shortly before the hearing. The administrative judges handle this in a variety of ways, some leaving it to the parties to resolve, some requiring a prehearing conference, and others issuing very specific pretrial orders setting dates for exchange of documents and for other aspects of the preparation for hearing.

The Hearing

The hearing is held on the record with a verbatim transcript being made of the proceedings, a copy of which is supplied to the applicant.[231] Department Counsel may make an opening statement followed by the applicant, who may also give an opening statement, delay it until after the government presents its case, or waive it.

The government has the initial burden of proof and presents its case first. It need only make a *prima facie* case before the applicant must go forward with the defense. Since the ultimate issue is "whether it is clearly consistent with the national interest to grant or continue [the applicant's] security clearance," and since "any doubt is to be resolved in favor of the national security and considered final," the government's burden to make a *prima facie* case is slight.[232]

Following the presentation of the government's case, the applicant has the opportunity to present witnesses and other evidence on his behalf. Not only must evidence be presented in response to the specific charges of the SOR, but equally important is to present evidence in mitigation and evidence of the applicant's character and standing in the community. Adjudications under DoD Dir. 5220.6 apply the "whole person" concept, and the directive itself requires that each clearance decision be a "fair and impartial common-sense determination based on all relevant and material information."[233] Also, each of the Adjudicative Guidelines lists circumstances and conditions that may mitigate the proscribed conduct.[234] While the administrative judge may find that the alleged conduct did occur, he may nevertheless find that, considering the mitigating evidence and character, it is clearly consistent with the national interest to grant or continue the clearance and rule in favor of the applicant.

DOHA procedures allow for the Federal Rules of Evidence (28 U.S.C. 1010 et. seq.) to "serve as a guide," but they are not slavishly followed.[235] Hearsay evidence is permitted, as in other administrative hearings, with consideration given to the weight to be afforded the evidence.[236]

Although an applicant is generally allowed to cross-examine witnesses and to examine documents and other physical evidence, an exception is made when the evidence or testimony to be offered by the government contains classified information or is from a confidential informant, or where the witness is unavailable due to death, severe illness or some other similar cause.[237] Before such evidence can be considered by the administrative judge, the DoD General Counsel must determine that such evidence is relevant and material and that failure to consider the information would be substantially harmful to the national security. In the case of a confidential informant, the head of the department or agency in possession of the informant's identity must certify that the disclosure of the

informant's identity would be substantially harmful to the national interest. Because such undisclosed evidence is so inimical to the fundamental due- process right to confront one's accuser, DOHA makes every effort to avoid its use. To the present, Department Counsel has never applied for permission to use an oral or written statement without giving the applicant the opportunity to cross-examine.[238]

If the applicant intends to use classified evidence, advance written application must be made to the administrative judge so that a secured facility and a cleared court reporter may be obtained. Use of classified evidence in a case involving a contractor's employee case is rare; it is more often used in cases involving military and government personnel. In the unusual case where classified evidence is submitted, every effort is made to write the decision in an unclassified form. In only one case has it been required to classify the final decision because reference to the classified evidence was unavoidable.[239]

An applicant can apply for restoration of lost earnings if there is a final favorable clearance decision concerning a clearance that had previously been denied, suspended, or revoked.[240] The applicant must show that the earlier action was as a result of the gross negligence of the Department of Defense and not due to the applicant's failure or refusal to cooperate. Reimbursement is not authorized for counsel's fees or costs related to the appeal to DOHA.[241]

The grant or denial of a clearance is an all-or-nothing matter. A clearance may not be denied at a higher level while retained at a lower level such as Secret or Confidential. Also, there is no authority to grant a conditional, deferred, or probationary clearance. Any request for time needed to undergo some form of treatment, or for a period of probation, to meet the criteria for holding a clearance, will be denied.[242]

At the applicant's request, hearings may be open to the public. DOHA proceedings are covered by the Privacy Act, and no information produced in the proceedings can be released outside the government. Even the contractor's security officer can receive only the ultimate result. Decisions are published with all identifying information redacted.

Appeal to the DOHA Appeal Board

Either the applicant or the government may appeal a decision of an administrative judge by filing a notice of appeal with the DOHA Appeal Board within 15 days of the judge's decision.[243] A written appeal brief must be filed with the Appeal Board within 45 days after filing the notice of appeal, citing the specific issues raised, and the specific portions of the record supporting the claimed error.[244]

The scope of review on appeal is whether: (a) the findings of fact of the administrative judge are supported by substantial relevant evidence; (b) the procedural requirements of Executive Order 10865 and DoD Directive 5220.6 were followed, or (c) the findings and conclusions are arbitrary, capricious, or contrary to law. In reaching its decision, the Appeal Board defers to credibility determinations of the administrative judge.[245]

The Appeal Board does not hear oral argument, as it construes the current Directive to preclude such authority. It may affirm or reverse the decision or remand the case to the administrative judge to correct an identified error. In doing so, the Appeal Board may specify the action to be taken on remand.[246]

Once the determination of the administrative judge is affirmed by the Appeal Board, it is final. Although judicial review is theoretically possible to challenge constitutional error, as a practical matter that is not a realistic consideration.[247] The courts will not review factual determinations in national security clearances. Because DOHA has been at this process for so long, there is virtually no likelihood of success of a constitutional "due process" argument based on procedural defects. The possibility of a constitutional challenge based on grounds yet to be discovered by a creative attorney, of course, always exists.

A final decision by the Appeal Board is not a permanent bar. After a year from the time the initial unfavorable decision becomes final, an applicant may reapply and, if appropriate justification is supplied, the clearance may be granted.[248] If necessary treatment is obtained, or if the proscribed activity, such as alcohol or drug abuse, is avoided during that time, the likelihood that the clearance will be reinstated will increase. The decision to reinstate is made by the Director of DOHA, but Department Counsel may participate in the determination depending on the nature of the original allegations.

There is a higher probability of a security clearance being denied without a hearing than with one. From 1992 to 1997 in cases decided without a hearing, a clearance was granted in 23 percent of the cases and denied in 77 percent. With a hearing, it was granted in 53 percent of the cases and denied in 48 percent.[249] A hearing probably does not fully account for the difference. Appellants with cases unlikely to succeed will more likely opt for a decision on the written record and not spend the time and money for a hearing. Also, once counsel is involved, there is a greater likelihood for a hearing than simply a submission of documents and a decision on the written record.

Sources for Research of DOHA Decisions

DOHA has never published in print either its administrative judges' or its Appeal Board decisions, but does make copies of both available for public inspection and copying at its headquarters in Arlington, VA.[250] The decisions are maintained in chronological loose-leaf binders and may be read and copied by advance appointment with the DOHA headquarters' staff or may be requested by mail.

In 1997, DOHA began posting its decisions on the Internet, and they are currently available from 1996 to the present. The URL address is *www.defenselink.mil/dodgc/doha/industrial*. The cases are posted, in full, in chronological order based on the date of the decision. A search engine allows for systematic research of the cases. The Appeal Board cases are indicated by the suffix "A" added to the case number. Decisions of the administrative judges are indicated by the suffix "H."

DOHA publishes in print two indices and a "case citator" each year. The first index is of all administrative judge and Appeal Board decisions arranged by the adjudicative criteria considered in the case. Each case listed gives a synopsis of the case, the case number and date of the decision. The second index is a supplement of Appeal Board decisions only. It is organized by the major principles of law discussed in the cases. The "case citator" is a numerical listing of all cases decided by the Appeal Board, giving the date of the administrative judge's decision, the date of the Appeal Board decision, and the final action taken. It does not, as the name would imply, give citations to later cases, so unlike other case citators, one cannot research forward to find later cases addressing the same point of law. The indices and the case citator are available without charge by writing to the Office of the Clerk, DOHA, PO Box 3656, Arlington, VA 22203.

CHAPTER 8

Use of the Polygraph in Security Clearance Investigations

Background and Current Practice

On March 31, 1998, a divided Supreme Court, in *United States v. Scheffer,* held that the results of a polygraph exam could be banned from use in a criminal trial by either side because there is simply no consensus that polygraph evidence is reliable. The court found that the scientific community and the state and federal courts are extremely polarized on the matter.[251] The Scheffer case resulted from a court martial in which the defendant had attempted to introduce the results of a polygraph in support of his testimony that he did not knowingly use drugs. The government in that case argued against its reliability. Five of the concurring and dissenting justices noted: "there is much inconsistency between the Government's extensive use of polygraphs to make vital security determinations, and the argument it made in that case stressing the inaccuracy of these tests."[252] The majority of the court found nothing inconsistent, however, in the polygraph's use by the government for personnel screening and as a tool in criminal and intelligence investigations because, it said, such limited out-of-court uses of polygraph techniques differ in character from, and carry less severe consequences than, the use of polygraphs as evidence in a criminal trial.[253]

The court noted that between 1981 and 1997, the Department of Defense conducted over 400,000 polygraph examinations to resolve issues arising in counterintelligence, security, and criminal investigations. Justice Stevens, in a dissenting opinion, supported its use by DoD because, he said, its polygraph operators were trained in its own Polygraph Institute, "which is generally considered the best training facility for polygraph examiners in the United States."[254] The Supreme Court's opinion has put to rest any argument against the continued use of this technique as a tool in national security investigations.

The courts are divided on whether to admit evidence obtained during a polygraph, some disallowing it on the basis that it is not scientifically valid, others leaving it to the discretion of the trial judge. The Supreme Court continues to leave the question of its admissibility to the individual courts, deciding only that a blanket exclusion in criminal proceedings is not unconstitutional.

In a criminal case, statements made during a polygraph exam are not admissible unless given voluntarily, because of the Constitutional protections of the Fifth and Fourteenth Amendments.[255] However, the denial of a security clearance or of access to classified information, or the denial or loss of employment because of the withholding of a security clearance, is not a criminal sanction, so the Fifth Amendment right against self-incrimination offers no protection even if a polygraph test is required as a prerequisite.

Use in Security Investigations

The use of the polygraph in security clearance investigations has a long and controversial history. Even before the *Scheffer* case, there was a well-reported divergence of opinion regarding its validity. The 1997 *Report of the Commission on Protecting and Reducing Government Secrecy* summarizes this divergence of opinion stating:

Senior officials from agencies that use the polygraph see it as a significant tool because of its utility in generating admissions of wrongdoing, either during the pre-test, test, or post-test period. The polygraph saves time and money, and it serves as a deterrent by eliminating some potential applicants from seeking a highly sensitive position in the first place. The polygraph examination is conducted before the background investigation, saving additional resources should the applicant be rejected as a result of polygraph admissions. According to a May 1993 NSA letter to the White House, over 95% of the information the NSA develops on individuals who do not meet federal security clearance guidelines is derived via voluntary admissions from the polygraph process.[256]

The report notes that not only do many senior Intelligence Community officials believe that the polygraph is useful, but they also believe that it is scientifically valid. It further notes the reservations that many others have for using the polygraph as a fact-finding tool stating:

Although the polygraph is useful in eliciting admissions, the potential also exists for excessive reliance on the examination itself. A related concern is that too much trust is placed in polygraph examiners' skills, creating a false sense of security within agencies that rely on the polygraph. The few Government-sponsored scientific research reports on polygraph validity (as opposed to its utility), especially those focusing on the screening of applicants for employment, indicate that the polygraph is neither scientifically valid nor especially effective beyond its ability to generate admissions (some of which may not even be relevant based on current adjudicative criteria).[257]

A 1989 Department of Defense Polygraph Institute (DoDPI) study found that 60 percent of subjects were incorrectly cleared in a test that measured the subject's knowledge or guilt of a crime. The results of this test concluded that the ability to identify those guilty or knowledgeable of a crime was significantly worse than chance.[258] The Supreme Court, in the *Scheffer* case, referred to various studies that placed accuracy from 50 percent to 90 percent.[259]

Use of the Polygraph by Federal Agencies

The use of the polygraph in federal personnel investigations was formalized in an interagency report dated July 29, 1966, with the concurrence by Memorandum of President Lyndon B. Johnson. The rules adopted then continue today.[260] An Executive Branch agency, which has a highly sensitive intelligence or counterintelligence mission directly affecting the national security, may use the polygraph for employment screening and personnel investigations. First, its use must receive approval of OPM, and then, its regulations governing the use of the polygraph must be approved by OPM. A later National

Security Decision Directive, NSDD-84, approved the use of the polygraph for screening individuals with access to code word information.[261]

The Presidential memorandum required that an agency's regulations must provide that the person to be examined be informed: (a) as far in advance as possible of the intent to use the polygraph, (b) of other devices such as voice recording that will be used simultaneously with the polygraph, (c) the effect the polygraph examination or the refusal to take it will have on eligibility for employment, (d) that a refusal to consent would not be made a part of the personnel file, (e) the characteristics and nature of the polygraph machine and examination and an explanation of its physical operation and (f) the procedures to be followed during the polygraph and the disposition of the information developed.[262] Agency regulations further must require that no polygraph examination be given unless the subject voluntarily consents in writing after having been informed of the above requirements that the questions asked be relevant to the inquiry. A number of federal agencies require applicants to undergo a polygraph exam as part of the hiring process for employment screening; they are the Central Intelligence Agency, the Defense Intelligence Agency, the Drug Enforcement Agency, the Federal Bureau of Investigation, the National Security Agency, and the National Reconnaissance Office.[263] A few positions in the Department of Justice Command Center also require preemployment polygraphs because of their access to cryptographic information. Positions having access to certain Special Access programs also require a polygraph. The White House, National Security Council, State Department, and Congress have not adopted polygraph screening. Even among the agencies that use the polygraph, the scope, methods, and procedural safeguards may diverge.[264]

Use of the Polygraph by the Department of Defense

The use of the polygraph for any Department of Defense program is governed by DoD Directive 5210.48, which states the DoD policy. DoD Regulation 5210.48-R implements that policy. This directive and regulation apply not only to the military departments but also to the Defense Intelligence Agency and the National Security Agency, components of DoD. They do not cover its use by the other agencies dealing with national security information, except to the extent that DoD personnel may be assigned or detailed to them.

A polygraph examination is mandatory for employment by or assignment to the DIA and the NSA, and for assignment or detail of DoD employees to the CIA.[265] It is also mandatory for employment, assignment, or detail to some DoD "Special Access Programs."[266] It may only be used for any other personnel security investigation to resolve serious credible derogatory information, and then only with the consent of the examinee.[267] Moreover, no adverse action may be taken solely on the basis of a polygraph examination that indicates deception, except upon the written finding by the Secretary or Under Secretary of Defense, or a Secretary of one of the military departments, that the classified information in question is of such extreme sensitivity that access under the circumstances poses an unacceptable risk to the national security.[268] In addition to the above uses, polygraph examinations are authorized by DoD in connection with security clearance matters only in certain situations. They can be used to supplement investigations of

federal felonies, of unauthorized disclosure of classified information or of alleged acts of terrorism. They can also be used to determine eligibility of foreign nationals for access to classified information, or when requested by the subject of a personnel security investigation, for exculpation with respect to allegations arising in the investigation.[269]

DoD Procedures for Administering a Polygraph

The procedures for administering polygraphs for DoD programs are specified in Part D of DoD Directive 5210.48-R. There is no requirement that a person undergo a polygraph for any reason; however, the refusal to do so may be a bar to employment by certain of the DoD agencies such as the DIA or NSA, or assignment to the CIA. It may bar employment in any Special Access Program.

The person to be interviewed must consent in writing, must be given timely advance notice of the time and place of the polygraph and of the right to have counsel pres??ent, and must be advised of the privilege against self-incrimination and of the right to terminate the examination at any time.[270] This information, however, is often given to the person being examined after he is already in the examining room - too late to be effective. The person, who may have traveled some distance to attend the examination, is placed in the position of having to reschedule, or worse in his own eyes, of appearing to be uncooperative and having something to hide. Frequently, given the timing and context, the person chooses not to have counsel, often to their later regret.

The DoD regulation spells out the exact manner in which the examination must be conducted. No relevant question may be asked during the polygraph examination that has not been reviewed with the person to be examined before the examination, and all questions must have a special relevance to the inquiry. Certain "validating" questions may be asked without prior disclosure to establish a baseline from which the examiners can judge the validity of the answers to the relevant questions. The probing of a person's thoughts or beliefs, or questions on subjects that are not directly relevant to the investigation, such as religious or political beliefs or beliefs and opinions about racial matters, are prohibited.[271]

The examining room where the test is conducted will generally contain only a desk in which the polygraph instrument is installed if an older mechanical model, or on which a modern computer version is placed. The modern version of the instrument consists of a computer which generates lines on a video screen, duplicating the lines drawn by a series of pens on a moving scroll of graph paper on the older mechanical versions.

In addition to the desk, the room will generally contain only a chair for the operator, and chairs for the person examined and his counsel. An observation room is normally adjacent to the examination room connected by a one-way mirror. The observation room will contain a speaker connected to the examination room and listening and recording devices to record the examination. The examination may be, but is not always, witnessed by another investigator from the adjacent room. It may be recorded.

The role of counsel is limited but important. Counsel may not answer for the person being examined, but that person and his counsel may adjourn to discuss a response before it is given. Of course, any adjournment during the questioning will be noted in the report of the polygraph operator. Counsel's presence is also important to advise on possible self-incrimination issues. Counsel can be in the examining room during the preliminary questioning and may sometimes be allowed to remain during the actual running of the polygraph. At other times counsel may be required to observe the actual testing through the one-way mirror connecting the adjacent room. Since all of the questions asked during the actual test will have been reviewed prior to the person being attached to the polygraph machine, there will have been ample time for counsel and the person examined to object to any question.

The presence of counsel cannot be overestimated. It has a restraining effect on overly aggressive polygraph examiners and a calming effect on the examinee. In the end, however, it will not create truthful answers out of deceptive ones, nor allow a dishonest person to "beat the machine." If legal counsel is retained, it should be as early as possible in the process so that counsel can advise on the necessity, if any, of taking the examination and on any areas of possible self-incrimination. In general, from an applicant's point of view, unless it is one of those circumstances where a polygraph examination is absolutely required, one is better off declining since a refusal to take one cannot be the basis for any adverse action or denial of a security clearance.

The National Security Agency also requires a preemployment polygraph as a condition of employment. It requires periodic five-year repolygraphs thereafter. The polygraph covers both life-style and counterintelligence issues. All polygraph examinations are tape-recorded. Copies of the recordings or transcripts of the recordings are generally denied to the employee or applicant if there is a decision to deny or revoke access to classified information. However, NSA reports that in rare instances where the decision to remove a clearance raises a direct challenge to what was said during the polygraph, the person appealing the decision has been provided with the relevant portions of the tape recording of the interview.

Use of the Polygraph by Other Agencies

The CIA requires polygraphs of all applicants and regularly repolygraphs all employees on a periodic basis. It does not allow counsel to be present during any part of the investigative process or during the polygraph. The agency feels that the presence of counsel makes the investigation more difficult and less productive. The CIA does not disclose transcripts of the polygraphs, all of which are recorded, and does not disclose the charts or the questions asked, as it believes that this would compromise its investigative methods.[272] If someone challenges the rejection of his clearance or access based upon the polygraph test, the CIA will review the polygraph results to consider the person's objections, but will not disclose the exact responses given by the individual.

On December 17, 1999, the Department of Energy adopted a polygraph examination regulation in response to charges of laxity in security at some of its facilities

handling nuclear materials and atomic secrets.[273] As of July 16, 2000, of the 800 polygraph examinations administered, all had passed.[274]

The Polygraph as Evidence in Administrative Appeals

Federal agencies deciding appeals of actions affecting employees deal with results of the person's polygraph exam in a number of ways. The Defense Office of Hearings and Appeals (DOHA), which decides appeals of security clearance decisions, has held that admissions by an applicant made during a polygraph examination may be admissible in evidence even though the results of polygraph examination are not.[275] Such "results" would include the polygraph charts and the polygraph operator's interpretation of those charts. The DOHA Appeal Board has held that Paragraph D.6 of DoD Directive 5210.48, which states that "no adverse action will be taken solely on the basis of a polygraph examination chart that indicates deception," does not bar the use in evidence of the applicant's admissions.[276]

Whether an applicant can use a nongovernment, private polygraph examiner to present exculpatory evidence is, at the time of this writing, uncertain. In a 1998 Initial Administrative Judge's decision, it was held that the report of a privately hired polygraph operator offered by the applicant was inadmissible.[277] The DOHA Appeal Board reversed that decision on September 3, 1998, holding that an applicant for a clearance may offer in evidence a polygraph report administered by a private polygraph operator, but has the burden of proving its admissibility.[278] On remand, the administrative judge declined to follow the Appeal Board's ruling, disallowing the report of the private polygrapher on the basis that the Appeal Board's decision did not comport with applicable DoD policy allowing only polygraph examinations conducted by federal agencies conforming to DoD standards.[279] On further appeal, the DOHA Appeal Board overruled the administrative judge's finding that the polygraph examination was prohibited by DoD regulation. The Appeal Board, however, held in this case the applicant had failed to show that his polygraph examination was reliable.[280] The effect of the Appeal Board's decision is to allow an applicant to present evidence of a favorable polygraph examination upon a proper showing of reliability. Government counsel in this case indicated that at the time of the hearing, there was a proposed revision to DoD Regulation 5210.48-R, "Department of Defense Polygraph Program," which if adopted would bar the use as evidence of an applicant-sponsored polygraph examination.

The Merit Systems Protection Board (MSPB), another federal agency which hears appeals of adverse employment actions, does allow the results of polygraph tests into evidence if a foundation is laid establishing the test's reliability. While finding that polygraph results may be admissible, the MSPB does not hold that the result of such tests must be accepted into evidence.[281] It leaves to the presiding official whether to admit the test and to decide what weight is to be given such evidence.[282] In a 1980 case, the MSPB listed a number of factors to be considered in determining the reliability of polygraph evidence. The rigorous test of "reliability" established in that case was substantially diminished in a 1997 case which allowed into evidence an investigator's summary of the results of a polygraph test given by someone else. The investigator's summary was of what he had found in the files of an earlier police investigation. The basis for admitting

the summary in the 1997 case was that it was a "public record or report" admissible under Rule 803(8) of the Federal Rules of Evidence. The MSPB held that the problem of "double hearsay" went simply to the weight, not the admissibility, of the evidence.[283]

The MSPB allows both the employee and the government to bolster its case with polygraph evidence, but tends to give more weight to tests which support the government's case than those which support the employee's version of the truth.[284] Use of polygraph evidence in MSPB proceedings has been affirmed by the Federal Circuit Court of Appeals, which has held that it is within the province of the presiding official's credibility determinations.[285]

CHAPTER 9

Central Security Investigation Indices

A frequently asked question is whether information about a person obtained by one agency during a security investigation is available to other agencies. The answer is yes. A central repository of information was first authorized in 1953 by Executive Order 10450. That order directed the Office of Personnel Management to establish a central security investigations index containing the name of all persons about whom a security investigation had been conducted. It also required for each such person, adequate identifying information and a reference to each department or agency that conducted the investigation, or suspended or terminated the employment of such persons.[286] That index is known as the Security Investigations Index (SII).

A similar index, known as the Defense Clearance and Investigations Index (DCII), is maintained by the Department of Defense. The DCII is the single automated central repository that identifies investigations conducted by DoD investigative agencies and personnel security determinations made by DoD adjudicative authorities.[287] Both the SII and DCII document investigations and federal employees, applicants for federal employment and on employees of firms working for the federal government under contract.

A third central repository of information is the FBI, which maintains files on all of its investigations and a central fingerprint file. All of these indices are checked at the beginning of any clearance investigation as part of the National Agency Check (NAC), the first step in any investigation.[288]

The Security Investigations Index (SII)

The Office of Personnel Management maintains the SII, a compilation of information on all investigations conducted under Executive Order 10450, as well as other OPM investigations.[289] The SII contains a record of the agency conducting the investigation; the reason for any subsequent dissemination of information, the date of the case, the name and social security number of the subject of the investigation, and other identifying data.[290] Files are maintained in this index for 15 years unless a case has resulted in substantially actionable issues such as an adverse adjudication or a debarment, in which case the file will be maintained for 25 years. OPM is now starting another database that will list all security clearances granted or revoked throughout the civilian agencies of the government, information not presently included in the SII. The new index appears to parallel the DCII (see Chapter 4.)

When an agency makes a request, OPM will conduct a search of the SII and will provide the requesting agency with information from the index as well as from any investigative files it maintains.[291] The requesting agency must notify OPM of any adjudicative action taken on the subject within 90 days of receipt of the file. Also, any agency conducting its own personnel security investigation must notify OPM of the initiation of the investigation and of the final adjudicative action.[292]

If OPM conducts an investigation and its search of the SII reveals that an investigation of the subject has previously been conducted, it must obtain a copy of the previous investigation for review.[293]

The Defense Clearance and Investigations Index (DCII)

The DCII, although operated and maintained by the Defense Security Service, is available to other federal agencies with adjudicative, investigative, or counterintelligence missions, and is used throughout the intelligence community. Certain agencies may be authorized to be "contributors" to the DCII, while others may be authorized to have "Read Only" access. The security requirements for both contributors and "Read Only" activities are the same.

Although the DCII is an unclassified system and contains only unclassified information, positions having a direct access to a DCII terminal are considered ADP-1 Critical Sensitive due to the sensitive nature of the information in the index. Individuals having access to the DCII terminals must, therefore, have a favorably adjudicated background investigation. Because of the sensitivity of the information, DCII terminals are afforded the physical protection normally reserved for classified information. The terminals must be in a locked, guarded, and alarmed area, and when operational, access to the terminals is limited to authorized persons.

When a DOD contributor to the DCII becomes aware of significant, unfavorable information about an individual about whom clearance or access information has been entered by another DoD component, it must immediately notify the other component and send it copies of all relevant information. Although the DoD regulation covers only Defense organizations, non-DoD organizations also use the DCII, and they are also notified by DoD of unfavorable information. They, in turn, notify DoD and each other of unfavorable information.

The DCII database consists of an alphabetical index of personal names and occupational titles. Personnel security adjudicative determinations are also maintained by the subject's name.[294] The database includes information not only from personnel security investigations, but also information from investigations conducted by DoD criminal, intelligence, and fraud activities. The indexed names are not only those of the subjects of investigations, but also of cosubjects, victims, and cross-referenced "incidental" subjects. For entries related to personnel security investigations, the DCII lists the clearance eligibility and access status of an individual and the presence of any adjudicative file.

Investigative data in the DCII includes all information resulting from an investigation, when an investigation was opened and when it was completed. Changes are made to existing files whenever appropriate.

"Adjudicative" data is entered on all personnel with access to classified information and on those performing sensitive duties. Specifically, an entry is made immediately upon the suspension of access; when an interim access has been authorized; immediately

following the grant, denial, or revocation of a clearance or access; and any new information received subsequent to any earlier clearance or access determination.

Although an adjudicative determination may be deleted two years after employment or clearance eligibility ends, the data is maintained in a historical file for a minimum of five years after deletion from the DCII.[295]

Release of information in the DCII is tightly controlled. All releases of information from a DoD to a nonDoD agency must be recorded. A contributor may only disclose DCII data originated by that contributor. Any requests by individuals for release of investigative reports or adjudicative files on themselves are handled as Privacy Act requests. The release of such information can only be authorized by the agency contributing that information.

CHAPTER 10

Sensitive Compartmented Information and Special Access Programs

There are only three levels of classification of national security information: Confidential, Secret, and Top Secret. Those levels define, respectively, information, the disclosure of which could reasonably be expected to cause "damage," "serious damage," or "exceptionally grave damage" to the national security. No other terms may be used to identify classified information.[296] Certain information, however, is deemed so important that greater investigative standards and controls are placed on the "access" a person has to such information. In that category is certain classified information dealing with intelligence sources, methods, or activities known as Sensitive Compartmented Information (SCI), access to which is governed by standards established by the Director of Central Intelligence (DCI). SCI is held throughout the government, but to a lesser degree than in the past. In the 1980s there were an estimated 800 SCI compartments in the Department of Defense. By 1997 that was down to roughly 300 compartments.[297]

There is another class of information that imposes higher safeguarding and access requirements than "normally required for information at the same classification level." Such information is held in programs known as Special Access Programs (SAPs).[298]

Sensitive Compartmented Information

The National Security Act of 1947 requires the DCI to protect "intelligence sources and methods from unauthorized disclosure."[299] Executive Order 12333 further requires the DCI to protect intelligence sources and methods and to issue appropriate directives to implement the Order.[300] From those authorities has emanated Director of Central Intelligence Directive No. 6/4 (DCID 6/4), *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information.*[301] DCID 6/4 defines Sensitive Compartmented Information as "classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the Director of Central Intelligence."[302] Neither the National Security Act of 1947 nor E.O. 12333 or any other Executive Order has defined what is a "source" or "method." The use of these authorities to sometimes classify not only closely held information, but also newspaper articles, public broadcasts, and other open information in the public domain has been the subject of frequent criticism.[303] However, the right of the CIA to classify such information has been upheld by the Supreme Court.[304]

The criteria under DCID 6/4 for approving an individual for access to SCI are the Uniform Adjudicative Guidelines issued by the Security Policy Board. They are incorporated as Annex C to DCID 6/4. In general, the person must be: "stable, trustworthy, reliable, of excellent character, judgment and discretion, and of unquestioned loyalty to the United States."[305] All exceptions to these standards must be "common sense determinations" that the risk to the national security "is manageable" in the specific case for which the exception is granted.[306] In arriving at the decision of whether to grant access, all

doubts must be resolved in favor of protecting classified information. The ultimate conclusion in every case must be that the granting of access is "clearly consistent with the interest of national security," using "an overall common sense determination based on all available information."[307]

The investigation conducted on an individual under consideration for access to SCI will conform to the Uniform Investigative Standards for Single Scope Background Investigations (SSBI) established by the Security Policy Board. (See Chapter 2.) These have been incorporated verbatim into DCID 6/4 as Annex A. "Quality Control Guidelines" for conducting the SSBI are included in DCID 6/4 as Annex B. These Quality Control Guidelines are broad directions to investigators concerning the scope of information sought.

Individuals considered ineligible for access to SCI will not, solely for that reason, be denied access to other classified information. Conversely, individuals who are authorized access to SCI under an exception to the requirements of DCID 6/4 will not, solely for that reason, be considered eligible for access to any other class of information. The person requiring access to SCI must be a U.S. citizen as, in general, must his family. An exception will be made for a family member only for compelling reasons where it is determined that the security risk is negligible.[308] The lack of U.S. citizenship of a family member may be a factor. If the person seeking the clearance has lived outside the United States for a substantial period of his life, that may prevent a complete investigation of the individual which would preclude the granting of access.

Except in extremely rare situations, a comprehensive background investigation will be conducted before access to SCI is granted.[309] (Temporary eligibility investigative requirements are more fully discussed in Chapter 2.) The CIA now uses Standard Form 86, Questionnaire for National Security Positions (sometimes called a Personal Security Questionnaire or PSQ) as the basis for beginning all investigations and no longer uses its own form.

Appeals of Adverse SCI Access Decisions

The past practice of the CIA under earlier versions of DCID 6/4 had been to deny almost all requests for an appeal and almost all requests for the reasons for denial of access. With the issuance of E.O. 12968, that was no longer possible. The procedures for appealing decisions denying or revoking access to SCI are now described in Annex D to the current DCID 6/4. They apply government-wide not only to the "intelligence community" but to every other agency or government entity dealing with SCI.[310] Every person considered for initial or continued access to SCI (except in Special Access Programs) can utilize those procedures. This includes government civilian employees, military personnel, employees of government contractors, and applicants for government or industry employment.[311]

The directive provides that the senior official of each Intelligence Community organization (the SOIC) or his designee may designate an individual to be the Determining Authority to decide cases regarding access to SCI.[312] The appeals procedures state the

law established by judicial decision, that the denial or revocation of access under the Directive will not be considered the denial of a constitutional property or liberty interest in any claimed right to access to classified information.[313]

The right to appeal does not begin until there has been a final decision denying or revoking access.[314] In the past, to avoid giving an employee notice of any problem, or any opportunity to appeal, many government security officers simply directed the sponsoring contractor or government organization to withdraw the employee's nomination for SCI access. In such cases, the employee never knew that access was not or would not be approved. Even if the employee did know, that person could do nothing to protest because he no longer had a "need" for access. That practice is no longer permissible. E.O. 12968 guarantees a right to appeal a decision denying access to any other classified information, including SCI, with the exception of Special Access Program information.

Although present CIA policy is to provide an appeal in every case of a denial of SCI access, it is reported that some contractors and some agencies are still following the former practice, despite the language of E.O. 12968 and the DCID 6/4. Contractor security officers will frequently, with no notice to the employee, withdraw their nomination for a position requiring SCI access to remain in the good graces of their government counterpart who can exercise great control over a contractor. While access can no longer be summarily revoked for persons already having an access, it can be suspended indefinitely. Since an appeal is available only after a final decision and there are no time limits on reaching a final decision, the person is simply assigned other duties during an indefinite suspension.

The appeal begins after a final decision is made and there is a stay of an access decision pending the outcome of the appeal. Thus, any uncertainty regarding a person's qualifications is resolved by preventing access unless and until the appeal establishes that an improper decision was made.

Under the appeals procedures of Annex D to DCID 6/4, an individual is to be given a comprehensive, written explanation of the basis for the denial of access in as much detail as the national security permits. Classified information is not disclosed. The person has opportunity to appeal to a three-member appeal panel and to appear personally at some point in the process.

Appeal procedures at the CIA itself are described in CIA Administrative Regulation AR-10-16.[315] Although E.O. 12968 and DCID 6/4 require only that an agency provide an individual the investigative file if asked, the CIA does provide the investigative file to CIA employees at the time it provides the written explanation. It will not provide any polygraph documents.[316] An applicant for employment or a contractor employee must still request the file, and to him, the CIA will only provide a redacted summary memorandum, deleting, among other information, the name of the deciding official even though Executive Order 12968 requires its disclosure.

Appeals procedures for CIA employees differ from those for applicants and for contractor employees. An appeal by a CIA employee goes to a higher-level panel than

one provided to applicants and contractors employees on the belief that employees already have access to secure information and, therefore, closer scrutiny must be given to determine whether their security clearance should be revoked. CIA employees are entitled to a personal appearance before a member of the security staff who is generally a GS-12 to GS-14 level employee. The recommendations of the staff member based on the personal appearance are reviewed by the Associate Deputy Director for Administration/Security. The final level of appeal is to an Appeal Panel comprised of the Agency Executive Director who chairs the Panel, the Associate Deputy Director for Operations for Counterintelligence, and the head of the employee's career service or office. The decision of the Appeal Panel is final.

For CIA applicants and contractor employees and applicants, the personal appearance is before a senior security officer not involved in the original revocations decision, and the appeal is to a lower-level panel. The chair of that Appeal Panel is the Director of Security for contractors, or a senior staff member of the Security Office for applicants. The other panel members are a counterintelligence representative or a human resources representative and the chief of the component office sponsoring the application for access.

Adjudication Guidelines under DCID 6/4

Previously, the Adjudication Guidelines used to determine the qualifications of a person allowed access to SCI differed in many respects from those adopted by DoD for granting a Confidential, Secret, and Top Secret. Now, the uniform, government-wide Guidelines adopted by the Security Policy Board are incorporated in DCID 6/4 as Annex B. Because the Director of Central Intelligence is a member of the Security Policy Board, those Uniform Guidelines were prepared to meet the stringent requirements for access to SCI. The Uniform Guidelines are discussed in detail in Chapter 6.

Special Access Programs (SAPs)

Special Access Programs (SAPs) are defined by E.O. 12958 as a "specific class of information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level."[317] A SAP is also defined by the DoD as any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information.[318] It is elsewhere defined by the DoD as a program or activity employing "enhanced security measures exceeding those normally required for collateral information at the same level of classification."[319] Such programs may impose additional or special clearance and adjudication procedures, investigative requirements, and material dissemination restrictions. They may also impose special lists of persons with a "need to know."[320]

The basis for the creation of Special Access Programs has been provided by a succession of executive orders and has been used to generally encompass not only DoD weapons programs, but also SCI programs and other programs within the Departments of Energy and State, programs for the protection of the President, for the continuity of government operations, and for covert actions operated from within the Executive Office of

the President.[321] Special Access Programs can concern research, development, and acquisition activities, or intelligence or military operations, and can be funded by one agency and managed by another. While some programs are publicly acknowledged, others are unacknowledged. For such programs, their very existence and purpose are classified and may not be disclosed to any person without authorized access to that program.[322] Among such unacknowledged SAPs, there are programs even more sensitive called "waived programs." Those are considered so sensitive that they are exempt from the standard reporting requirements to Congress and are made known only to the Chairperson and Ranking Minority Member of the appropriate Congressional Committee with oversight authority.[323]

There are approximately 150 DoD-approved SAPs currently in operation, down from about 200 in the late 1980s.[324] Because of the lack of accountability, central oversight or coordination of such programs, and because of the especially high cost of security for such programs, E.O. 12958 requires an annual review and validation of all SAPs.[325] That review is carried out in DoD by the Special Access Program Oversight Committee (SAPOC) and within the Intelligence Community by the Controlled Access Program Oversight Committee (CAPOC).[326]

Executive Order 12958 for the first time formalized the requirements for the establishment of Special Access Programs. Unless authorized by the President, they can be created only by the Secretaries of Defense, State, and Energy, and the Director of Central Intelligence. These officials are directed to keep such programs "at an absolute minimum." They are to limit such programs to those in which the number of persons having access "ordinarily will be reasonably small."[327] When SAPs are applied to the creation of major weapons systems such as a new bomber, or major facilities such as an unacknowledged air base, the term "reasonably small" becomes quite elastic.

Before a SAP can be established, there must be a specific finding by the appropriate Secretary or the Director of Central Intelligence that: (a) the vulnerability or threat to the information is exceptional and the normal criteria for determining eligibility for access to such information are not sufficient to protect it from unauthorized disclosure, or (b) the program is required by statute.[328]

In the Department of Defense, the classification and protection of SAP information are controlled by DoD Regulation 5200.1-R.[329] A SAP may only be initiated by the Secretary or Deputy Secretary of Defense, and then not until the appropriate Defense Committees of Congress are notified and 30 days have elapsed after notification is received.[330] Every SAP must be assigned an unclassified "nickname," and may also have a classified "code word" or words.[331] A nickname is a combination of two unclassified words, while a "code word" is a single word.[332]

For DoD SAPs there are cases where the mere knowledge of a particular contract or its association with a SAP is classified. In those instances the agencies normally performing functions associated with the Industrial Security Program, such as the Defense Security Service for personnel or facility security, or the Defense Contract Audit Agency for financial review, may be "carved out," i.e., relieved of their normal responsibilities.

Those functions will then be performed by the sponsoring component-level SAP Central Office. In those cases, a written security plan including security review procedures must be prepared for that particular SAP.[333] If a SAP is terminated or placed in a lower classification status, it becomes "de-sapped."[334]

The type of background investigation to be conducted for each of the various types of Department of Defense SAPs is specified in DoD's Personnel Security Program Regulation.[335] If the Special Access Programs involve SCI, Presidential support activities, duties associated with nuclear weapons, North Atlantic Treaty Organization information, or "Single Integrated Operational Plan-Extremely Sensitive Information" (SIOP-ESI), the nature of the personnel background investigation required to authorize access is specifically stated in the Uniform Investigative Standards which may be supplemented by the DoD Regulation. For any other SAP the special investigative requirements in excess of the minimum requirements are established on a program-by-program basis depending on their sensitivity.

Appeal of SAP Access Decisions

There is no appeal required by statute or executive order of a denial or removal of access to a SAP. However, E.O. 12968 encourages the use of the appeals procedures authorized for other types of classified information.[336] *Green v. McElroy,* which is the basis for any "due process" procedures in the Industrial Security program, suggested that the President might have inherent authority to deprive a person of his employment in this area so long as it was done explicitly.[337] This suggestion was adopted and applied to contractor employees by Executive Order 10865, § 9, and DoD Directive 5220.6, Paragraph B.6. It was also applied to government employees by Executive Order 12968.

It is not required that there be appeals of SAP access decisions. However, they may nevertheless be permitted (or, in the case of DoD, required) by agency regulation. If allowed they may differ from the procedures for appealing decisions denying access to SCI or to nonSAP programs.[338] Any such special procedures for DoD programs must be approved by the Secretary or Deputy Secretary of Defense.[339]

Although a person whose previously granted access was revoked would know of the loss, there would be no appeal, as such decisions, either for government and contractor employees, are entirely discretionary with the program administrator. A person who had not previously been approved for access would, in most cases, never know that he was considered and rejected for SAP access, or even that a program-access request had been conducted.

The denial or loss of access to a SAP will not, of itself, cause a loss or denial of any clearance at the Confidential, Secret, or Top Secret level. However, the underlying conduct that was the basis of the SAP denial may also be a basis for the loss of a collateral clearance. Before such further loss of a collateral clearance could occur, the affected individual would have all appeal rights associated with that type of clearance—if for a contractor employee it would include the right to a full hearing, or for a government employee or applicant or member of the armed forces, the right to personal appearance.

CHAPTER 11

Physical Security, Facility Clearances, and the NISPOM

The protection of national security secrets is like a three-legged stool: one leg is proper identification of the information, i.e., classification; the second is control of persons with access, i.e., personnel security; and the third is physical protection of the information, i.e., safeguarding. Each leg is necessary, or the security stool collapses. This chapter discusses physical security.

As discussed in Chapter 1, until a few years ago each department and agency, and frequently subunits within the departments, had its own requirements for safeguarding classified information. Each had regulations which were as particular as specifying the type of safe that was required to protect a particular item. Contractors doing business with different agencies of the government had to meet different requirements to protect the same type of information.

In April 1990, the President directed the National Security Council to explore the development of a single, integrated industrial security program that could result in cost savings and improved security protection. This resulted in a report from the Secretaries of Defense and Energy, and the Director of Central Intelligence that recommended the establishment of a National Industrial Security Program.[340] They reported that 21 departments and agencies each had their own industrial security program — in the Department of Defense alone there were 47 different standards, manuals, and directives supplementing the basic executive orders and legislation. This diversity created a significant burden on both industry and government, and the increased cost was passed on to the government. The report found that standardization could reduce duplication by at least 20 percent.[341] It recommended that a National Industrial Security Program be created under the direction of the Department of Defense, with the Secretary of Energy continuing to have the authority to protect nuclear materials and the Director of Central Intelligence the authority over Sensitive Compartmented Information. From those recommendations came a government-wide consolidation of physical industrial security requirements known as the National Industrial Security Program (NISP).

On January 6, 1993, Executive Order 12829 was issued, formally establishing the National Industrial Security Program which was to serve as a single, integrated, cohesive program to safeguard federal government classified information released to contractors and to licensees and grantees of federal agencies. The program is mandatory for all Executive Branch departments and agencies. The executive order directed the National Security Council to provide overall policy direction, the Information Security Oversight Office (ISOO) to oversee the implementation of the executive order, and the Secretary of Defense to issue a *National Industrial Security Program Operating Manual* (NISPOM). Specific requirements were to be prescribed by the manual for safeguarding classified information by contractors, licensees, and grantees during all phases of the contracting process. The Secretary of Energy and the Chairperson of the Nuclear Regulatory Commission were given responsibility for that portion of the manual dealing with nuclear

energy, and the Director of Central Intelligence was made responsible for the portion dealing with intelligence sources and methods, including Sensitive Compartmented Information. A NISP Advisory Committee, consisting of representatives of both government and industry, was also established under the executive order to consider policies under the NISP and recommend changes to it.

Executive Order 12829 concerned only the safeguarding of information released to government contractors but not the broader problem of safeguarding government-held classified information, a far greater amount of information. That problem was addressed two years later by the issuance of Executive Order 12958 on April 17, 1995, which prescribed a uniform system for classifying, declassifying, and safeguarding information applicable to both government and industry.[342] Parts 1, 2 and 3 of the executive order concern the classification and declassification of information. Part 4 addresses safeguarding the information, i.e., measures and controls to protect classified information. The Security Policy Board was directed to draw up recommendations for the handling, storage, distribution, transmittal, destruction of, and accounting for classified information.[343]

The National Industrial Security Program Manual (NISPOM)

The NISPOM was issued in January 1995 under the mandate of Executive Order 12829.[344] A supplement was issued in December 1994, providing enhanced security requirements for Critical Restricted Data (RD), Special Access Programs (SAPs), Sensitive Compartmented Information (SCI) and other compartmented programs that protect intelligence sources and methods.[345] The NISPOM replaced *the DoD Industrial Security Manual for Safeguarding Classified Information* previously in use. It applies not only to DoD but to all Executive Branch departments and agencies and cleared contractor facilities.

Under the NISPOM, every contractor must appoint a Facility Security Officer (FSO) to supervise security measures implementing the manual. The FSO also must be cleared as part of the facility clearance. Written contractor procedures may be required by the government security office monitoring the contract but are not required in every case.[346] Periodic security reviews are conducted, normally on advance notice, to the contractor. Unannounced reviews may be conducted at the discretion of the government.

Contractors are required to continually review their security procedures and to report any security infractions. To ensure that contractors do so, security hotlines also are maintained by the concerned government agencies so that contractor employees can directly report any security irregularities to the government. Contractors must inform their employees of the availability of these hotlines.[347]

Stringent reporting requirements are imposed on the contractor.[348] Any concerns of possible espionage, sabotage, or subversive activities must be immediately reported in writing to the FBI. Information of a less-serious nature must be reported to the Cognizant Security Agency. This includes "any adverse information" coming to the contractor's attention concerning any of its cleared employees, such as suspicious contacts or evidence

that an employee no longer wishes to work on classified matters. Also to be reported are changes affecting the facility clearance such as a change in ownership, change in storage capability, the discovery of classified information the contractor is not authorized to have, or actual or suspected compromise or loss of classified information. Contractors must also establish a system of "appropriate administrative and disciplinary action" to be taken with respect to employees who violate the NISPOM. Any such discipline must also be reported to the government.[349]

Facility Clearances

A facility clearance is an administrative determination that a company is eligible for access to classified information or for an award of a classified contract.[350] Facility clearances are registered centrally by the government, and valid clearances are now fully and mutually recognized by all federal departments and agencies, a great step forward from the days when each agency conducted and issued its own facility clearance. A contractor cannot apply for his own clearance, but must be sponsored by a government agency, either before or after the award of a classified contract.[351]

To be eligible for a facility clearance, a contractor must (a) have need for access to classified information in connection with a government requirement; (b) be organized under the laws of one of the states, the District of Columbia, or Puerto Rico; (c) be in the United States or its territories or possessions; (d) have a reputation for integrity and lawful conduct of its business and not be barred from participating in any U.S. Government contracts; and (e) not be under foreign influence, ownership, or control such that the granting of the facility clearance would be inconsistent with the national interest.

The senior management official and the facility security officer must also be cleared to the level of the facility clearance. Officers, directors, and senior managers who are excluded from holding a clearance must be specifically designated by the organization's board of directors or executive body. Where there are multiple facility locations, the home office must have a facility clearance at least to the highest level of any of the cleared facility locations. If there is a parent-subsidiary relationship, the parent must generally have a clearance at least equal to any cleared subsidiary. Where a parent facility can be excluded from a need for access to classified information, it will not be granted a clearance.[352]

It is the contractor's responsibility to request personnel clearances for only those employees for whom access to classified information is essential to their work. This request must be kept to a minimum, and requests to establish "pools" of employees are prohibited. If an employee is cleared by one agency, the contractor need only submit identifying data to the new agency to verify the clearance without having to request an entirely new investigation and clearance. Contractors are no longer permitted to grant clearances.[353] Clearances granted to former government employees may be converted to industrial clearances, and previously terminated clearances may be reinstated without a new background investigation if no more than 24 months have elapsed and there is no known adverse information.[354]

Foreign Ownership, Control, or Influence (FOCI)

The determination of whether a company is under FOCI is the responsibility of the Defense Security Service and is done on a case-by-case basis. It entails the balancing of the United States' interest of encouraging foreign investment in this country with the need to ensure that foreign firms cannot undermine United States security by having access to critical technology and classified information.[355]

A U.S. company under FOCI is ineligible for a facility clearance. However, efforts may be taken to isolate or quarantine those foreign interests to permit the company to continue doing classified government business. The government may impose restrictions and controls on a company short of removing its facility clearance to preclude the unauthorized disclosure of classified information within the company.[356] Subjective factors are considered, such as the type and sensitivity of the protected information and the company's record of compliance with U.S. law. Additionally considered are whether nonU.S. citizens hold management positions, or the ownership of 3 per cent or more of the company's voting securities, or 25 percent of a particular class of stock, or 25 percent of nonvoting securities.[357] Details of loan arrangements between the company and a foreign person, details of financial arrangements that allow a foreign person to demand repayment, interlocking offices and directorships by foreigners, and any other factor demonstrating a capability of a foreign interest to influence the operation or management of the company are also factors in determining whether there is FOCI.[358]

When a company holding a facility clearance enters negotiations for a proposed merger, acquisition, or takeover by a foreign person, the government must be notified with all details of the transaction. If it is determined that a company is under FOCI, the primary consideration is the safeguarding of classified information.[359] If it is determined that the company is under FOCI, the facility clearance will be suspended until protective measures are implemented. Where it appears that foreign influence or control may occur, the company will be asked to submit a "negation plan," providing positive measures to prevent foreign persons from obtaining access to classified information. Such a plan may include a voting trust agreement and proxy agreement where the voting rights of the foreign citizen are vested in cleared U.S. citizens who can act on corporate matters without control by the foreigner.[360]

The government may require a Special Security Agreement imposing industrial security and export control measures on the company. It may also require a Technology Control Plan prescribing security measures necessary to preclude access by nonU.S. citizens to classified information. Failure of the company to ensure compliance with any approved security arrangement may be grounds for revocation of the facility clearance.[361] A sample FOCI Special Security Agreement is found at Appendix I.

Physical Safeguarding of Classified Information

Both the NISPOM and the DoD Information Security Program Regulation go into great detail on how classified material is to be safeguarded.[362] Not only do the regulations prescribe how documents and physical objects are to be protected, they also give detailed

procedures for preventing oral discussions from being overheard or intercepted.[363] End-of-the-day security checks and perimeter controls over entry points are mandated.[364] Contractors (but not government agencies) are required to maintain an accountability system for Top Secret documents, with each document being numbered and inventoried.[365]

Documents must be stored in approved safes or filing cabinets meeting specified GSA requirements, and Top Secret documents must have supplemental protection such as intrusion detection systems, security guards, or "security in depth."[366] Control of safe combinations and approved methods of repair are also specified.[367] If the volume of classified material is large, an entire area of a room, floor, or building may be designated as a Closed Area. These areas must be built to meet specific requirements with approved intrusion detection devices, and access to them is limited to authorized personnel with appropriate security clearances and need-to-know for the classified information.[368] Uncleared visitors in such areas or those without the need-to-know must be escorted at all times.

The methods for transmission of classified material are also specified in detail in both the NISPOM and the DoD Information Security Program Regulation.[369] Marking, packaging, method of shipment, designation of authorized carriers, modes of electronic transmission, use of couriers or escorts, and the use of commercial passenger aircraft are all specified in great detail.[370]

Reproduction and disposition of classified documents are also specified in detail for contractors and to a much lesser degree for government users.[371] For contractors, rec??ords of all copying of Top Secret documents must be maintained for a period of years. At the end of their need, classified documents held by contractors must either be returned to the government agency providing them or be destroyed by approved methods of pulverizing, burning, or other methods that totally disintegrate the documents. The destruction must be witnessed, for Top Secret Documents by two witnesses, and recorded.[372] These requirements for witnesses and recording do not apply to government users. Nevertheless, government employees still have accountability for Top Secret documents.

Automated Information Systems

Protection of classified information on automated information systems (AIS), i.e., computers, has become one of the most significant areas of concern to the government, particularly with the frequent reports of "hackers" trying to break into classified government systems. The NISPOM states in only the briefest detail directions for AIS security. The contractor must promulgate an AIS Policy and an AIS Security Plan and must appoint an Information Systems Security Representative to implement the policy and plan and to maintain contact with the contracting agency.[373] These responsibilities include ensuring physical safeguards for the AIS equipment and ensuring that access to it is only by authorized personnel. Security measures must be implemented for the use of the AIS equipment and for its repair and maintenance. Protection of AIS used for Sensitive Com-

partmented Information and Special Access Programs is controlled by the NISP Supplement, Chapter 8.

Presumably, government buildings and installations are inherently more secure than contractor facilities, requiring less control of individual items of equipment in those locations. For government users of AIS, the regulation states only that activities using such equipment must adopt security procedures that will prevent unauthorized access, will ensure the proper removal and destruction of machine parts containing classified information, and will ensure that equipment is inspected by cleared personnel before being removed from protected areas.[374]

Many types of common AIS equipment, such as computers and printers, emanate electronic signals that can be intercepted from a distance and interpreted to determine what information is being generated on those systems. The government program to investigate and prevent the interception of such signals is known as TEMPEST.[375] When it is determined that classified information may be exposed to TEMPEST collection, it is the responsibility of the government contracting authority dealing with the contractor to perform threat assessments and vulnerability studies. If necessary, the government may provide TEMPEST shielding and TEMPEST-shielded equipment, with all costs associated with such measures being recoverable as a direct charge to the contract.[376]

The protection of the information systems themselves is a vast and continuing government undertaking, a detailed discussion of which is beyond the scope of this book. Authority for the protection and regulation of information systems is found in the Computer Fraud and Abuse Act of 1986, the Computer Security Act of 1987, and in OMB Circular A-130, Management of Federal Information, Appendix III, Security of Federal AISs. This is an area of concern of the National Telecommunications and Information Systems Security Office and the National Computer Security Center. Their publications, and those of the DoD and the Director of Central Intelligence on the subject, are compiled in Appendix A, *Sources on the Protection of National Security Information.* The protection of such equipment on a national scale has been addressed in a 1998 Presidential Decision Directive 63, *Protecting America's Critical Infrastructure.*[377]

The DoD Information Security Program Regulation implements not only Executive Order 12958 for classified national security information but also prescribes procedures for protecting sensitive information that is not classified but which requires some type of protection or control.[378] Among such information is that exempt from disclosure under the Freedom of Information Act (FOIA) which the regulation designates as "For Official Use Only" (FOUO).[379] The regulation also creates a category of "Sensitive But Unclassified" (SBU) information described as also being exempt under FOIA, but the regulation does not spell out how that information differs from "FOUO."[380]

Also included as protected information under the DoD Regulation is Drug Enforcement Administration Sensitive Information, DoD Unclassified Controlled Nuclear Information, sensitive information under the Computer Security Act of 1987, i.e., "unclassified information that could adversely affect the national interest or the conduct of Federal programs," and "technical documents."[381] Although the DoD regulation carefully

states that its requirements apply only to national security information, it suggests the use of "controls and protective measures" to prevent the disclosure of other such unclassified information.[382]

CHAPTER 12

Security Clearances at the National Security Agency

Legal Authority for the NSA Security Program

Although the National Security Agency is an agency of DoD, because of the highly sensitive nature of its intelligence and cryptographic activities, higher security standards are applied for obtaining or keeping employment there. Policies and procedures specifically addressing NSA personnel security are governed by P.L. 86-36, "NSA Officers and Employees;" P.L. 88-290, "NSA Personnel Security Procedures;" Executive Orders 10450 and 12333, DoD Directive 5210.45, "Personnel Security in the National Security Agency,"[383] and DoD 5200.2-R. The use of polygraph examinations, which are generally limited for employment purposes in the DoD, is required for initial or continued access to sensitive compartmented information (SCI) at the NSA.[384]

No person may be employed by, detailed to, or assigned to NSA unless his access to the agency's classified information is "clearly consistent with the national interest."[385] Employment depends on the successful outcome of a full-field investigation. While a person can be provisionally employed pending the outcome of the investigation, he may not have access to sensitive cryptologic information until the investigation is successfully completed.[386] The full-field investigation may be temporarily waived if the Director of NSA personally determines in writing that such an action is clearly consistent with and advisable in the national interest.[387]

All NSA affiliates must be eligible for access to SCI which is governed by the standards and procedures of DCID 6/4. NSA has issued implementing procedures for adjudicating denials or revocations of access or security clearances in accordance with E.O. 12968 and DCID 6/4.[388] The NSA regulation covers not only NSA employees, but also "affiliates," which collectively refers to applicants for employment, contractors, consultants, and experts. The adjudication procedures provided by the NSA regulation have a particular importance to employees of the agency. Since access to SCI is mandatory for employment at NSA, a revocation of access means automatic processing for termination of employment.

Each year about 25 new applications for access are denied, and one or two accesses by current holders are revoked. Because a decision to deny or revoke SCI access means denial or loss of employment, NSA takes particular care not to use the access review process as a substitute for procedures for handling disciplinary problems. Decisions to use one or the other process are made centrally by senior human resources personnel in consultation with personnel from the Office of Security to ensure that employees whose performance is not viewed favorably by unit managers are not removed by using the more summary security access procedures.

Preemployment Security Review

Preemployment screening of an applicant requires not only a full-field background investigation, but also a polygraph examination and a psychological examination. Since a full- field investigation is the most expensive and time-consuming part, the hiring process is divided into two phases. An applicant, after completing a personal security questionnaire, is first given a polygraph examination covering counterintelligence, serious crimes, and drug use. Counter-intelligence issues concern whether the person being examined has ever engaged in or has knowledge of espionage against the United States, has ever been approached to sell or has sold classified materials to unauthorized persons, or has had unauthorized contacts with a representative of a foreign government.[389] The applicant will also be given a psychological examination by an NSA psychologist. If the first phase is successfully completed, a background investigation will then be initiated.

Investigations of NSA employees and of military personnel working at NSA are conducted by the Defense Security Service. There is only one standard for access, and no higher standards exist for any of the various compartments at NSA. Once employees are cleared for SCI access, all other determinations are based on a need-to-know. Interim appointments are rarely granted, and if so, for only a short period.

Appeals of Adverse Security Determination

An employee or affiliate who has been denied access or whose access has been revoked is entitled to the procedures provided under NSA/CSS Reg. No. 122-07.[390] That Regulation implements the requirements of Executive Order 12968 concerning access to sensitive cryptologic information, to include SCI. For an employee, notice of the decision to revoke access also serves as notice of the proposal to remove the employee from federal service at NSA.[391] Debarment from NSA facilities while an appeal is pending poses no great problem with respect to an applicant or a contractor's employment. However, current employees who appeal an access decision are entitled to remain on the federal payroll until the appeal is decided. In those cases, they may be placed on administrative leave if unclassified duties are unavailable.

The Chief, Adjudicative Services, is responsible for the initial decision to deny or revoke access and for providing written notice of the decision and proposal to remove the employee whose access has been denied. A review of the initial decision, if requested by the employee or affiliate, will be made by the Chief, Adjudicative and Security Information Services. If a review is not requested, the determination of the Chief, Adjudicative Services, is final. In the case of an employee, a referral will be made to the Assistant Director for Support Services (ADS) or designated Deciding Official for a decision regarding the proposal to remove the employee from employment.[392]

The decision to deny or revoke can be appealed to an Access Appeals Panel (AAP) appointed by the ADS. The AAP shall consist of at least three but not more than five voting members and shall include one minority and one female member.

When a determination has been made to deny or revoke access, the employee or affiliate will be provided as comprehensive and detailed a written explanation of the basis for determination, suitably redacted to protect classified information on which the decision is based. The person will also be provided with notice of the right to be represented by counsel at his own expense, to request the entire investigative file, to request a review of the decision, and to appeal if the review of the decision is sustained.[393] NSA's policy is to immediately provide the investigative file with the notice of the decision. Written replies and requests for review must be postmarked within 45 days from the date the employee or affiliate receives the decision to deny or revoke access. In the case of an employee, the notice to revoke access also serves as a notice of proposed removal from employment by NSA. The failure to request review will result in a referral to the ADS proposing termination of employment.

A review of the decision to deny or revoke access will be made by the Chief, Adjudicative Services. In a request for review at that point, an employee may submit only written materials. If the Chief, Adjudicative and Security Information Services, sustains the initial decision, the employee or affiliate may appeal that decision within 30 days to the Access Appeals Panel. The employee or affiliate may appear in person before the panel, with or without a representative who may be an attorney, to make a personal presentation and present "relevant documentation and material information, but shall not present or question witnesses."[394] The panel will consider "any new information provided in writing or in person, by the employee or affiliate." New information may be subject to verification and adjudication. The panel may request additional agency support personnel to be present to assist at the hearing.[395]

The decision of the panel to sustain or not to sustain the denial or revocation of access will be based on a majority vote of the members and will be final. In the case of a "senior" employee, the panel makes only findings of fact and a recommendation. It is the Director of NSA who makes the final decision.[396]

The employee or affiliate will be provided with a final written decision specifying the reasons on which the decision was based, and for veterans-preference eligible employees, advising of the right to appeal to the MSPB.[397]

NSA formerly had another statutory avenue available for removing an employee whom it considered to be a security threat. Former Section 303 of Public Law 88-290 permitted the Secretary of Defense to terminate the employment of any officer or employee of NSA when he: (a) considered such action to be in the interest of the United States, and (b) determined that the procedures in other provisions of law authorizing termination could not be invoked consistent with the national security.[398]

CHAPTER 13

Department of Energy Security Clearance Program

The Department of Energy's (DOE) Security Program

DOE operates its security program under the authority of the Atomic Energy Act of 1954, as amended (AEA), and Presidential executive orders to protect nuclear-related information, materials, and facilities and national security information.[399] The origins of DOE's security program date back to the Manhattan Engineer District, the World War II project that developed the atomic bomb. The authority to protect nuclear-related information devolved from it to the Atomic Energy Commission, then to the short-lived Energy Research and Development Administration (ERDA), and from there to DOE. The Nuclear Regulatory Commission (NRC) was created at the same time as ERDA to regulate the civilian nuclear power industry and is responsible for security regulations pertaining to its employees and to the civilian nuclear power and fuel fabrication industries.[400]

The AEA established particular requirements for the protection of nuclear-related information. Those requirements are the bases for 80 to 90 percent of all classification decisions now made by DOE.[401] The AEA provides for the classification of information covering the "design, manufacture or utilization of atomic weapons...the production of special nuclear material...or the use of special nuclear material in the production of energy," all of which are collectively termed "Restricted Data" (RD).[402] Such information is classified from origin and is often referred to as "born classified."

When information which relates primarily to the military use of atomic weapons can be safeguarded as defense information, it may be removed from the RD category and becomes known as "Formerly Restricted Data" (FRD).[403] Declassifying this type of information by DOE must have the concurrence of the Department of Defense. FRD, like National Security information classified an executive order, can be classified as Confidential, Secret, or Top Secret.[404] It is protected in the same way as National Security information. However, dissemination of classified FRD information to foreign countries is strictly controlled.[405] In that case, FRD reverts back to its status as Restricted Data.

DOE's personnel security program implements not only the AEA but also the requirements and standards of Executive Order 10450, Executive Order 10865 pertaining to government contractors, and Executive Order 12968 pertaining to government employees and applicants. The DOE criteria and appeals procedures are identical for both its employees and its industrial contractors. Unlike the separate procedures afforded by DoD and other agencies dealing with National Security information, DOE's employees and applicants, like their industrial counterparts, have the right to a full administrative hearing when their access authorization is in question.

DOE has its own separate system authorized under the AEA for granting "access authorizations," which is similar to that of other agencies that grant Confidential, Secret,

and Top Secret clearances or SCI access. Most DOE employees receive either a "Q" access authorization equivalent to Top Secret, or an "L" access authorization equivalent to Confidential or Secret.[406] A "Q" access authorization permits an individual to have access, on a need-to-know basis, to Top Secret, Secret, and Confidential levels of Restricted Data or Formerly Restricted Data, and to National Security information or information concerning Special Nuclear Material. An "L" access authorization permits an individual to have access, on a need-to-know basis, to Confidential Restricted Data, Secret, and Confidential Formerly Restricted Data, and to Secret and Confidential National Security information. Access to classified information marked as "COMSEC," "CRYPTO" or "SCI" at any classification level requires a "Q" access authorization.[407]

The majority of DOE access authorizations are granted to DOE contractors and subcontractors. The number of persons with DOE access authorizations has declined steadily since 1988, to now almost half the 1988 number. Most of the drop is attributable to a reduction in "Q" access authorizations. In 1988 there were 150,000 "Q" access authorizations and 50,000 "L" access authorizations. By June 1998, that number had dropped to 70,000 "Q" access authorizations and 40,000 "L" access authorizations.

The number of cases under administrative review has also dropped in like proportion. In 1995 there were 222 cases closed. Of those, 103 reviews were withdrawn before decision, and 93 clearances were either denied or revoked. Only three were granted. In 1997 of a total of 99 cases, 41 were canceled without decision, 54 were denied or revoked, and only 1 was granted. The figures for the first half of 1998 are consistent.[408]

Of accesses denied or revoked between 1995 and 1998, 30 percent were for falsification, 25 percent were for alcohol use, 19 percent were for drug use, 5 percent were for alcohol and drugs, 7 percent were for mental health problems, and 13 percent were for reasons of mental health with substance abuse. There were no revocations under any of the other criteria in those years.[409]

DOE Policy and Regulations

The criteria for determining DOE access eligibility are found at Title 10, Code of Federal Regulations, Part 710, Subpart A. That regulation also provides the procedures for administrative review when unresolved questions remain concerning a person's eligibility for access authorization.

DOE regulations cover access to both classified matter and to Special Nuclear Material, i.e., plutonium, uranium enriched in isotope 233 or 235, or other "specially determined materials" but not "source materials."[410] They apply to employees and applicants for employment with DOE, to agents or contractors of DOE,[411] and to "access permittees," i.e., individuals whom DOE has permitted to have access to Restricted Data applicable to civilian uses of atomic energy.[412]

DOE background investigations for access eligibility are conducted by OPM and the FBI and are as vigorous as those of any other agency. DOE may conduct additional inquiries, such as personnel security interviews and mental evaluations by medical

examiners to determine access eligibility. Unlike procedures in other agencies, the investigative process itself may be challenged during the investigation if an employee or applicant believes it is inappropriate as, for example, a belief that a mental examination is unwarranted. If an individual declines to undergo such inquiries, the processing of the access authorization will be suspended, or in the case of a person already holding authorization, administratively terminated. The suspension or termination may be appealed to the Director, Office of Safeguards and Security, by filing a written appeal within 30 days of the investigative action. After inquiry, the Director, DOE Office of Safeguards and Security, must determine whether the particular inquiry was appropriate.[413] If the Director determines that it was not, he will direct the process for access authorization to continue or order the access authorization be reinstated without the objectionable line of inquiry.

DOE prohibits the threat of loss-of-access eligibility to coerce or retaliate against anyone exercising his rights under any statute, regulation, or DOE policy. It provides that any officer or employee of DOE violating that policy will be subject to disciplinary action.[414] DOE regulations prohibiting such actions are explicit. Its policy, however, has not always been followed in practice, as shown by a number of newsworthy cases reporting on nuclear power plant contractors who retaliated against their whistle-blower employees.[415]

Remedies for retaliation by nongovernment managers are found in the federal whistle-blower laws.[416] DOE contractor employees who believe that they are being subjected to a review or investigation in retaliation for whistle-blowing are advised to contact the DOE Office of Contractor Employee Protection, a unit of the DOE Office of Inspector General. DOE employees with similar claims are advised to report such treatment or actions directly to the DOE Office of Inspector General.[417]

DOE regulations grant to government employees more rights during the review of access determinations than are required by Executive Order 12968. They do not, however, conform to the executive order in every respect.[418] DOE is at the time of this writing revising its regulations to conform to the executive order. It is expected to retain the additional procedural safeguards for its employees now in its regulations beyond those required by the executive order.[419] New rules are forthcoming in 2000.) On December 17, 1999, DOE adopted a polygraph examination regulation in response to charges of laxity in security at some of its facilities handling nuclear materials and atomic secrets.[420] As of July 16, 2000, of the 800 polygraph examinations administered, all had passed.[421]

DOE Access Criteria

The criteria for determining eligibility for access to DOE-protected information under the Atomic Energy Act are essentially the same as those used by other Executive agencies to protect National Security information and Sensitive Compartmented Information. Those criteria include consideration of treason, terrorism, or involvement with the unconstitutional overthrow of the government; family members in countries with interests inimical to those of the United States; falsification or misrepresentation during the access investigation; failure to safeguard classified information or to follow regulations;

serious mental illness, drug, or alcohol abuse; financial irresponsibility; criminal behavior; or other conduct demonstrating dishonesty, unreliability, or untrustworthiness or that the individual may be subject to duress or exploitation.[422] The specifically listed criteria are not considered exhaustive and DOE may consider any information that in its judgment raises a question about an individual's eligibility for access.

DOE's regulations, like those of other agencies, specifically state that any access authorization will be made based on a comprehensive, common sense judgement considering all relevant information, both favorable and unfavorable. Such information includes the seriousness of the conduct; the surrounding circumstances; the frequency and recency of the conduct; the individual's age, maturity, motivation, and voluntariness at the time of the conduct; the potential for rehabilitation or reformation and the potential for pressure and duress on the individual.[423]

DOE Adjudicative Guidelines

When DOE revised its personnel security regulations in 1994, they included Adjudicative Guidelines interpreting the criteria for the grant or continuation of access to material classified under the AEA and to special nuclear material. They are similar to Security Policy Board's Uniform Guidelines in that they addressed the "Concerns," the "Disqualifying Factors" and the "Mitigating Factors for each criterion."[424] The criteria in the 1994 DOE Guidelines are: (a) allegiance; (b) relatives; (c) falsification; (d) security/safeguards responsibilities; (e) emotional, mental and personality disorders; (f) refusal to testify; (g) alcohol abuse; (h) drug abuse; and (i) honesty, reliability and trustworthiness (including criminal behavior, deviant sexual activity, foreign preference, financial irresponsibility, and violation of commitment). The guidelines also address discrimination in the workplace (EEO) and whistle-blower concerns.

DOE states that it now follows the Uniform Adjudicative Guidelines issued by the Security Policy Board. However, its regulations have not yet been revised to reflect this.[425] In reviewing DOE adjudicated cases, those issued prior to the adoption of the Uniform Guidelines may be of more limited precedential value than those decided based on the new guidelines.

DOE's 1994 Adjudicative Guidelines differ in many respects from the Security Policy Board's Uniform Guidelines.[426] The DOE version contains guidelines on "relatives," "refusal to testify" and "violation of commitment" not found in the Security Policy Board's Uniform Guidelines. DOE's guidelines are far more specific, giving the adjudicator less flexibility, a format that is abandoned in the Security Policy Board's Uniform Guidelines. For example, DOE's mitigating factors regarding drug abuse state that mitigation will be considered if: (a) the drug abuse was within the past 12 months, but was only an isolated incident or of infrequent enough incidents to warrant acceptance of the individual's assurance that he will not be involved with the drug while holding a DOE access authorization; or (b) the drug involvement was more than 12 months ago, and the individual is willing to offer assurance that he will not be involved with drugs while holding DOE access authorization. The Security Policy Board's Uniform Guideline for mitigation of drug abuse, by contrast, is simply that the drug involvement "was not re-

cent," "was an isolated or infrequent event," that there is a demonstrated intent not to use drugs in the future, and that there has been a satisfactory completion of a drug treatment program.

Another difference in the guidelines is that DOE has a criterion of "violation of commitment" for which the disqualifying factors are violating the terms of a DOE Drug Certification form, or violating "any commitment or promise made to DOE or any other agency or department of the federal government upon which DOE previously relied to favorably resolve an issue of access authorization eligibility." Such an inflexible criterion is difficult to rationalize, unless meant to serve as a "last chance agreement" for a person with prior infractions. If that is its purpose, DOE can use it to avoid readjudicating an access eligibility for repeat offenders.

The DOE guidelines admonish its Personnel Security Specialists not to make moral judgments and not to determine an individual's guilt or innocence, but to compare the information available on an individual with the DOE guidelines to decide whether the person is an acceptable security risk. The Personnel Security Specialists are advised to note and evaluate all derogatory information about the individual on a Case Evaluation Sheet to be maintained in the Personnel Security File (PSF). The DOE guidelines further note that the PSF will be available to the individual, either through the administrative review procedures or the Privacy Act, and advise the Security Specialists not to include any references to sources that have provided information or testimony under a pledge of confidentiality. They advise the Security Specialists that the PSF is unclassified and no longer considered as "sensitive," "For Official Use Only information" and that it may be released on written or verbal request of the concerned individual.[427]

Although the DOE guidelines admonish the adjudicators not to make "moral judgments," the Guidelines themselves seem to do so. For example, "disqualifying" sexual activity is defined as sexual activity that is "criminal in nature (regardless of whether the individual has been, or is being, prosecuted for the commission of such acts)." Activities so broadly described can create a variety of problems. In some states, sex between consenting adults of the same gender is illegal, while in other states sex between unmarried consenting adults of the opposite gender is illegal. In still other states, certain sexual acts between consenting adults of the opposite sex who are married to each other are illegal. Another disqualifying factor is the "commission of sexual acts for money or other reward," an activity that is legal in some states. Under the DOE guidelines, it becomes virtually impossible for adjudicators to make determinations without making moral judgments.

The DOE Adjudicative Guidelines enforce the agency's concern for reprisals for whistle blowing and for other protected activity, such as EEO complaints. Appendix A to the DOE guidelines establishes numerous levels of oversight in the security review process designed to prevent reprisals. It notes that adjudications will be in the Office of Hearings and Appeals, a separate DOE activity. It advises Security Specialists to be aware of conduct by DOE managers and contractors which might indicate that there was not truly a security concern but indicate that the managers or contractors simply want to

be rid of troublesome employees. The DOE guidelines emphasize the importance of determining the motivation of supervisors who are proposing to remove an employee.

The Review and Appeals Process

The review and appeals process is the same for DOE employees, applicants for DOE employment, contractor applicants, and contractor employees. If an investigation reveals substantially derogatory information, the Director of Security of the local DOE field office will review the information and may conduct further interviews, require a mental evaluation, or use other means the Director deems appropriate to further investigate. If the local Director of Security is still not satisfied that access is appropriate and that the derogatory information is unresolved, the matter will be referred to the Manager of the field operation or to the Director of the Office of Safeguards and Security, for Washington, DC, area cases. Ultimately, all unresolved cases will be referred to the Director of the Office of Safeguards and Security who will make the final determination whether to grant access or to institute administrative review procedures.[428] At that point an individual may request a hearing on the record.

Within 30 days after it is determined to institute an administrative review, the individual is provided a "notification letter" stating the reasons why substantial doubt exists concerning his eligibility for access authorization, "which shall be as comprehensive and detailed as the national interest permits."[429] The individual may choose to have a determination on the written record or a hearing before a Hearing Officer who must be a DOE attorney or a senior management official appointed by the Director, Office of Hearings and Appeals.[430] At any hearing the individual has the right to counsel who, for DOE employees, may be a union representative. DOE counsel will represent the department.[431]

The Hearing Officer has much broader powers than an administrative judge in the Defense Office of Hearings and Appeals (DOHA), most importantly, the power to issue subpoenas for witnesses and documents.[432] The Hearing Officer may administer oaths and take sworn testimony, sequester witnesses, and control the dissemination or reproduction of any record or testimony including correspondence, documents, and information in computerized systems held by the subpoenaed person.[433] Unlike DOHA hearings which are open unless requested to be closed, all DOE hearings are closed except to DOE Counsel and the individual and his counsel, unless authorized to be open by the Hearing Officer.[434]

The individual may testify and present witnesses and other evidence on his behalf. All witnesses are subject to cross-examination. DOE regulations impose an affirmative duty on DOE Counsel not only to represent the department, but to assist the Hearing Officer in developing a full administrative record in bringing out a full and true disclosure of all facts, both favorable and unfavorable.[435] Although formal rules of evidence do not apply in DOE hearings, the Federal Rules of Evidence serve as a guide to assure the production of the most probative evidence. That evidence must be material, relevant, and competent. Hearsay evidence is admissible "for good cause shown" and is afforded as much weight "as the circumstances warrant."[436]

Only in certain instances may oral or written statements of government witnesses be received without allowing the opportunity to cross-examine. The first is when the head of the agency supplying the statement certifies that the person providing the statement is a confidential informant engaged in gathering intelligence information, and that the disclosure of his identity would be harmful to the national interest. The second is when the Secretary of DOE or his designee determines that (a) the information is reliable and material and failure to receive it would be harmful to the national interest; and (b) the person could not appear to testify due to death, illness, or similar cause or "due to some other specified cause determined by the [supplying agency's] head to be good and sufficient."[437] Classified records may also be put into evidence without showing them to the individual if (a) the Secretary of DOE or his designee determines that the records are material to a controverted issue, and the failure to consider such evidence would be harmful to the national security; and (b) a summary of the records or evidence is made available to the individual "to the extent that the national security permits."[438]

The Hearing Officer may request the local Director of Security to conduct a further investigation on unresolved issues. A written transcript of the proceedings must be made and furnished to the individual without cost.[439] At the close of the hearing, the Hearing Officer will render an opinion with findings of fact and reasons supporting those findings. Only if the Hearing Officer determines that the grant of continued access to protected information "would not endanger the national defense and security and would be clearly consistent with the national interest" can he find in favor of the individual. The possible impact on any DOE program by the loss of an individual's access authorization may not be considered by the Hearing Officer.[440]

Either DOE or the individual may appeal an unfavorable decision to the DOE Office of Hearings and Appeals within 30 days after receipt of the decision. The record is not necessarily closed at the completion of the administrative hearing. The Director, Office of Hearings and Appeals, may initiate an investigation of any statement made in the request for review, may solicit and accept submissions, i.e., briefs from either side, and "may consider any other source of information that will advance the evaluation" so long as both parties are allowed to respond to the third party submissions.[441] Within 45 days after the final close of the administrative record the Director, Office of Hearings and Appeals, will make specific findings based on the record of each issue on appeal. If the Director finds that it "would not endanger the national defense and security and would be clearly consistent with the national interest," he will render an opinion in favor of access authorization or reinstatement. If he cannot, an opinion will be rendered denying or revoking access authorization.[442]

Where a decision is based on testimony of witnesses whom the individual has not been allowed to cross-examine, only the Secretary of DOE may make a final determination denying or revoking access authorization. After the case is closed, an individual may request reconsideration, but only if there is a new *bona fide* offer of employment requiring access and there is either relevant and material new evidence of which the individual was not previously aware, or there is convincing evidence of reformation and rehabilitation.[443]

Sources of DOE Authority and Precedent

Since 1994, decisions of the DOE Office of Hearings and Appeals have been published and are available on the Internet at *www.oha.doe.gov/persec2.htm.* They are published in full (with personal identifying information redacted) including the date, number of the decision, name of the hearing officer, and any subsequent determinations affirming or overruling. The Web site has a search engine that allows the cases to be searched both by adjudicative criteria and by key words. The decisions are "linked" to other cited cases simplifying legal research.

DOE regulations and adjudicative criteria, including all updates, may also be found on the Internet at *www.oha.doe.gov/persec1.htm.* This Web site also contains a list of questions and answers for the general guidance of persons with questions about their access determination.

CHAPTER 14

Department of Justice and the Federal Bureau of Investigation Security Clearance Program

Department of Justice (DOJ) Security Program

All positions at DOJ are categorized at various levels of sensitivity from Special-Sensitive to non-Sensitive, but not all require national security clearances. Positions requiring access to Top Secret national security information or SCI are designated Special-Sensitive. Those positions with access to Secret or Confidential information are Critical-Sensitive.[444]

The Assistant Attorney General for Administration is the designated senior agency official for national security matters and is responsible for the overall national security information program of DOJ.[445] Functions concerning classified national security information have been delegated to a designated Department Security Officer, who presently is the Director, Security and Emergency Planning Staff. Implementation of the security program has been further delegated to the Security Program Managers of each of DOJ's components.[446] A Department Review Committee has been established to resolve all issues dealing with classified information except its compromise and questions concerning the eligibility of persons for access to such information.[447]

The Director, Security and Emergency Planning Staff, as the Department Security Officer, has the authority to grant, deny, suspend, or revoke an applicant's or employee's access to classified information.[448] That responsibility has been redelegated to the Security Programs Manager (SPM) of five of the DOJ components which initially determine an employee's eligibility for access to classified information.

Clearances for DOJ Employees and Applicants

As required by Executive Order 12968, DOJ regulations provide appeal procedures for government employees and applicants for government employment for whom it has been determined do not meet the standards for access to classified information. Under the regulations, such persons are to be provided a comprehensive, detailed, written explanation of the bases for denial of access and 30 days in which to request the records on which the denial or revocation was based. The regulations further require that the records be provided within 30 days to the extent such documents would be provided if requested under the Freedom of Information Act or the Privacy Act and to the extent that the national security interest and other laws permit.[449] Upon receipt of that information, an applicant or employee may file a written reply to the initial deciding authority and, if unsuccessful, request review and reconsideration of the adverse determination.[450] The initial deciding authority is either the Director, Security Planning Staff, or the designated Security Program Manager who has been delegated the responsibility for making eligibility determinations.

If a component agency such as the FBI, the Drug Enforcement Administration, or the United States Marshals Service denies or revokes a security clearance, an appeal of that decision may be taken by the applicant or employee to DOJ. Reconsideration may first be requested to the authority that revoked the clearance prior to the appeal to the ARC. The employee will be provided with a written notice of the final decision and reasons for the decision. If the decision is adverse, there will also be notice of the right to appeal that decision.

If the denial or revocation of eligibility for access to classified information is sustained, a further and final appeal may be taken by the affected individual within 30 days to the DOJ's Access Review Committee (ARC).[451] The ARC consists of three members, who are presently an Deputy Assistant Attorney General, the Counsel in the Office of Intelligence Policy Review, and a Deputy Assistant Attorney General for Human Resources.[452] There are no security professionals on the committee.

Executive Order 12968 and implementing DOJ regulations provide that an applicant or employee may "request the opportunity" to appear personally before the ARC and to present relevant documents, materials, and information.[453] There is no provision for presenting witness testimony or for cross-examining any persons who gave information upon which the department's adverse decision was based. At a personal appearance before the ARC, an applicant or employee may be represented by an attorney or other representative of the employee's choice, but at his own expense.[454] Although Executive Order 12968 permits agencies to provide additional review procedures beyond those required by the executive order, DOJ has not done so.[455]

In any appeal to the ARC, the Department Security Officer or designated SPM Program Manager may present relevant written information and, if the applicant or employee appears personally, may also appear personally. Only if the ARC determines that it is consistent with the national security may written submissions by the Security Officer be shown to the appellant, or may the appellant be present during a personal presentation of the Security Officer.[456] Also, the Attorney General may bar any particular procedure under DOJ's regulations from being made available to an appellant if it would reveal classified information. The Attorney General may dispense with the appeal procedure entirely, if it cannot be invoked "in a manner consistent with the national security."[457]

A decision of the ARC is discretionary. Access to classified information will be granted only where the ARC determines that access is "clearly consistent with the national security interests of the United States."[458] Unless the Attorney General requests recommendations from the ARC and personally exercises appeal authority, the ARC's decisions are final.[459]

Procedures for appeal are spelled out in a brief, two-page statement issued by the ARC.[460] They provide that appeals filed outside the 30-day time limit for appeal will not be accepted, unless there are "compelling reasons" beyond the appellant's control to prevent timely filing. The ARC may request additional information from the appellant, from the Department Security Officer, or from any other source. Personal appearances will take place at the Main Department of Justice Building. If the appellant is an employee,

travel expenses and reasonable per-diem costs for the appearance will be born by the employing DOJ component. For applicants, contractors and appellant's representative, travel and other costs are the responsibility of the appellant.

No recording or transcription of the personal appearance before the ARC may be made other than those approved by the ARC. Statements are not made under oath, and there is no right to present or cross-examine witnesses. Only the appellant, his personal representative, the Department Security Officer, or designated representative and its counsel are permitted to attend. Unless the ARC requests further supplementation, the record will be closed at the conclusion of the appellant's personal appearance. As of August 1998, the ARC had decided three cases with two more pending.[461]

DOJ regulations concerning the standards for access to classified information essentially repeat the requirements of Executive Order 12968. They require that a person must meet the standards for eligibility for access in accordance with the executive order, have a demonstrable need-to-know, and sign an approved nondisclosure agreement.[462] An employee granted access to classified information must also provide written consent permitting access to his financial records maintained by a financial institution and access to his credit reports and records pertaining to travel outside the United States.[463] Such information may be requested by DOJ only if it has reasonable grounds to believe that the employee or former employee may be illegally disclosing classified information to a foreign power or has incurred excessive indebtedness or acquired unexplained affluence or had the capability or opportunity of disclosing classified information when such information is known to be lost or compromised to a foreign power.[464]

Clearances for Contractor Employees

Matters under the industrial security program affecting facility and contractor clearances (except personal service contracts) are referred to the Defense Security Service for investigation and approval.[465] An appeal of a proposal to deny or revoke a security clearance of a contractor's employee is heard by the Defense Office of Hearings and Appeals. (See Chapter 7.) If a clearance is granted and DOJ does not agree with that decision, the department may deny the person access to its information.[466] This DOJ policy appears to conflict with the requirements of Executive Order 12968 which, for contractor employees as well as government employees, refers not to clearances, but to "eligibility for access to classified information." For a contractor employee to be cleared for access to classified information but denied access to the facility where the information is located, appears to subvert the purpose and intent of the executive order.

Small personal service contractors, such as court reporters or persons providing services directly to the courts under the Classified Information Procedures Act, are investigated and cleared directly by DOJ.[467] As noted above, the ARC allows only a personal appearance and does not permit the presentation or cross-examination of witnesses. Limiting contractors to a personal appearance appears to be contrary to Executive Order 10865 governing contractor employee appeals, which gives such persons the right to a full hearing including presenting witnesses and cross-examining the government's witnesses as occurs at DOHA. The rights provided by Executive Order 10865 are expressly

preserved by Executive Order 12968, § 7.2(c). At the time of this writing, there have been no contractor appeals to the Access Review Committee.[468]

Polygraphs

Preemployment polygraphs are not required for anyone in DOJ, except 12 of its employees in the Justice Command Center who have access to cryptological information. Polygraphs are used by several components of DOJ. The FBI uses them for preemployment investigations of its entire staff, and the Drug Enforcement Administration uses them for its intelligence research analysts and special agents.

Sensitive Compartmented Information

DOJ acts under delegated authority from the CIA regarding the safeguarding of Sensitive Compartmented Information. DOJ has the authority to grant or suspend SCI access. If derogatory information is adduced, an employee's or applicant's appeal is under the procedures provided by the CIA in DCID 6/4. (See Chapter 10.)[469] DOJ follows the requirements for the physical protection of SCI found in DCID 1/21.

The Federal Bureau of Investigation (FBI)

The FBI, although a component of DOJ, has a security clearance program far larger than its parent department.[470] The FBI accounts for approximately 10 percent of the security clearance investigations of the entire federal government.[471] All of its employees are required to hold a Top Secret clearance, regardless of whether they handle national security information.[472] Unlike most nondefense agencies whose security clearance investigations are done by OPM, the FBI does all of its own. The investigations are done, for the most part, by former or retired FBI agents as part of the Background Investigation Contract Service (BICS).

The FBI also conducts background security investigations for individuals needing access to classified information under the Classified Information Procedures Act (CIPA) (see Chapter 16), the Foreign Intelligence Surveillance Act of 1978 (FISA), and nonFBI members of Joint Task Forces. It also conducts investigations for others needing access to FBI facilities and classified information, such as attorneys representing FBI employees in personnel matters, staffs of Federal Independent Counsel, Special Consultants, Federal Legislative and Judicial Branch personnel, and chaplains and doctors counseling or treating FBI staff.[473] The FBI unit dealing with personnel security is divided into three sections, one section handling clearances for FBI employees including those with SCI clearances, a second section handling clearances for contractor employees, and a third dealing with clearances for persons who are not employees or contractors, but who need access to FBI facilities, such as police officers or attorneys.[474]

FBI regulations governing security clearance investigations are found in its Sections 67, 259, and 260 of the FBI *Manual of Investigative Operations and Guidance* (MIOG). Further requirements are described in its *Manual for Administrative Operating Procedures* (MAOP).[475] Section 67 of the MIOG deals with the investigative requirements for applicants for FBI employment and prescribes how such investigations are to

be conducted. Investigative procedures described under Part 260 for contractor personnel are quite different.

FBI Employees and Applicants

Executive Order 12968 requires agencies to limit their requests for access eligibility to only those with a demonstrated foreseeable need. It prohibits them from requesting or approving eligibility in excess of actual requirements. However, it excepts agencies from that limitation where eligibility for access is a mandatory condition of employment.[476] The FBI is one of those agencies. The FBI's rationale is that it is a "reactive" agency that frequently has to respond to emergencies requiring security clearances. It asserts that it must be able to easily transfer personnel among assignments, some of which may require dealing with classified national security information. For that reason, FBI requires all of its employees to have a Top Secret security clearance regardless of whether they have access to national security information.

The standards for adjudicating access decisions affecting FBI employees are apparently listed in the MAOP. They are described as detailed and particular, similar to the former Department of Defense adjudicative standards previously found in its regulation, DoD 5200.2-R. For example, the FBI standards addressing "experimental" or "regular" drug use specify the precise number of times and the recency of use for each type of illegal substance. In contrast, the much more general Adjudicative Guidelines now used throughout the government state that any drug use is disqualifying, but allows mitigation for events that are "not recent," "are isolated," or are "an aberration event."[477] The more general guidelines give greater latitude to the adjudicating authority to consider individual circumstances, but there is less certainty in the outcome.

Like the DOJ, the FBI makes two determinations for each applicant and employee, trustworthiness and suitability, the former being determinative of eligibility for a security clearance. A trustworthiness investigation is not begun until the applicant has been determined to be suitable. Security investigations of FBI applicants are concerned with character, loyalty, reputation, and associations.[478] Where derogatory information obviously disqualifies the applicant, the investigation is ended. Various FBI indices are checked, not only on the applicant, but on the applicant's close relatives, references, roommates, close social friends, and others with whom the applicant has been closely associated during his adult life. Former spouses are interviewed, and if the applicant is to be married, the future spouse and future immediate relatives are also investigated. Organizations listed by the applicant are also checked against FBI indices. Neighbors and roommates for the past five years are interviewed, and if derogatory information is developed, the interviews continue to the indefinite past.[479] References and neighbors are questioned not only about the applicant but about the applicant's close relatives and associates. If derogatory information is developed, inquiries are made to "informants and reliable sources."[480] If allegations of disloyalty or subversive activities are received, appropriate security informants are contacted.[481]

All employments, including part-time and of any duration, are verified, and periods of unemployment must be accounted for. Supervisors and a representative number of

coworkers are interviewed. Law enforcement records are checked in detail on both the applicant and close relatives. Credit checks are done for seven years, and if bankruptcy is admitted, checks go back 10 years. Persons interviewed are questioned about the applicant's lifestyle and whether he appears to be living beyond apparent means.

The background investigation of applicants for employment is a lifetime check going back to age 18. Records before age 18 or juvenile records are not checked. The FBI investigation exceeds the Uniform Investigative Standards for the Single Scope Background Investigation (SSBI) which requires a check of criminal records for only the prior 10 years, and employment for only the prior seven years.[482] Because of that, applicants for FBI employment are required to submit the FBI's own form, FD-140, rather than a Standard Form 86, because the SF-86 requests information going back only 10 years. FBI questionnaire form FD-814 is used for five-year reinvestigations.

The FBI both investigates and adjudicates the security clearances of its employees and applicants for employments. An appeal of the FBI's decision to deny or revoke a security clearance or access to SCI may be taken by the individual affected to the Department of Justice for adjudication under its procedures as described earlier in this chapter. Reconsideration may first be requested to the initial decision authority in the FBI. If the FBI's decision is sustained, a further and final appeal may be taken to the DOJ Access Review Committee.

FBI Employment Polygraphs

All applicants for FBI employment are polygraphed.[483] Polygraphs are not used for reinvestigations, except for certain assignments dealing with espionage cases. All employees detailed to the CIA are repolygraphed. FBI regulations provide that failure to submit to a polygraph or to cooperate is not an automatic disqualifier but may be considered with other factors in determining whether an individual should be hired.[484] The regulations do not state what other factors might be considered.

Employees of Contractors with the FBI

The FBI is, by agreement between DOJ and DoD, a user agency of the Defense Investigative Program. Under that agreement the FBI conducts the investigations of employees or applicants of contractors doing business with the FBI after which they are referred to the Defense Security Service (DSS) for an adjudication, and if warranted, for the granting of a clearance by the DSS.[485] They include persons working on contracts for the construction or modification of FBI facilities, for installation or servicing of equipment, and vendors with access to FBI offices and consultants.[486] These personnel investigations are covered by Part 260 of the MIOG. In certain cases contractor clearances may be sought from the DOJ rather than DSS, for example, for Special Investigators for the FBI's Background Investigation Contract Service. In those cases the completed FBI investigation will be presented to the DOJ Security Officer for an adjudicative determination.[487] If there is an unfavorable determination, the case will be referred to the Defense Office of Hearings and Appeals for an administrative hearing. (See Chapter 7.)

Under current FBI regulations, a determination of trustworthiness for contractor employees will be made in accordance with the standards set forth in Department of Defense Regulation 5200.2R, Appendix I, "Adjudication Policy – General."[488] These are the Uniform Adjudicative Guidelines approved by the White House on March 24, 1997.[489] Notwithstanding that a prospective contract employee has the requisite DSS clearance, the FBI can conduct its own trustworthiness investigation and determine whether to place the contract employee in a FBI project.[490] If a clearance is granted by DSS, and the FBI does not agree with it, like DOJ (as described earlier in this chapter), FBI will deny the individual access to its facilities.[491] The FBI can also remove a contract employee from an FBI project if it determines that his employment is not in the best interest of national security.[492] As noted above, this policy appears to conflict with the requirements of Executive Order 12968 which address "eligibility for access" to classified information, both for government employees and for contractor employees and applicants. To be granted a clearance for access to classified information but denied access to the facility where the information is located, appears to subvert the purpose and intent of the executive order.

Contractor employees apply for a clearance by submitting a Standard Form 86, "Questionnaire For Sensitive positions" and two copies of an FD-258, "Applicant Fingerprint Card."[493] Contractor employees or applicants are not generally polygraphed but may be in the case of a specific project requirement.

Because the FBI is concerned with any non-bureau employee having access to its facilities, information, or employees, anyone, even if not dealing with national security information, must be investigated and cleared for access to FBI facilities.[494] For example, people in this category are electrical, plumbing, or vending machine service personnel and cleaning workers. For individuals with only "escorted" access, only a limited background investigation is conducted, but for persons having "unescorted" access to FBI facilities, a SF-86 must be submitted and a 10-year background investigation conducted.[495] Determinations of eligibility for facility access for such persons are made by the Security Program Manager taking into consideration criteria set forth in Executive Order 10450 and DCI/D 6/4.[496]

Facility Clearances

As noted in Chapter 11, a facility clearance is an administrative determination that a facility is eligible, from a security standpoint, for access to national security information. The FBI refers all facility clearance investigations to the Defense Security Service and relies on the DSS to conduct the appropriate inspections, issue the requisite facility clearances, and do follow-up monitoring.[497] Requests by the FBI, like any other contracting agency, are made to DSS by submitting a Form DD 254. Facility clearance requirements are those specified by the NISPOM. (See Chapter 11.) There may be circumstances where the FBI's Contract Security Officer may wish to exclude all or a portion of a project from DSS inspection, which is known as a "carve out." In such event, the Security Officer must certify at least once a year that the project has been inspected and meets appropriate security requirements.[498]

CHAPTER 15

Removal from Government Employment for Security Reasons Under 5 U.S.C. § 7532

5 U.S.C. § 7532 provides a summary procedure for removing from government employment a person considered to be a security risk. This section was intended to be invoked "only where there is an immediate threat of harm to the national security in the sense that the delay from invoking normal dismissal procedures could cause serious damage to the national security."[499] It applies only to positions that are directly connected to the nation's safety, i.e., those concerned with protecting the nation from internal subversion or foreign aggression, as distinguished from those concerned only with the general welfare.[500] The summary process under Section 7532 is available only to certain agencies that are particularly concerned with military and diplomatic affairs, i.e., the Departments of State, Commerce, Justice, and Defense, the military departments, the Coast Guard, the Atomic Energy Commission, the National Aeronautics and Space Administration, the National Security Agency, the Defense Intelligence Agency, and the National Imagery and Mapping Agency (formerly the Defense Mapping Agency).[501]

Summary procedures available under 5 U.S.C. § 7532 are not intended to replace other statutory avenues for removing a government employee, either for general or for security-related considerations. Their use is not mandatory even where national security considerations are the basis for removal. The general personnel laws also may be used to remove an employee for "cause" when there is a reasonable doubt as to loyalty.[502] The language of Section 7532 is permissive, and even though a removal could be taken under that section, it was not intended to preempt the procedures available under 5 U.S.C. § 7513 or other statutes.[503] For example, NSA may rely on the National Security Act of 1959 or the Act concerning NSA Personnel Security Procedures to effect a person's removal.[504]

The summary process under Section 7532 differs in several respects from Executive Order 12968 which provides government-wide procedures for revoking an employee's access to classified information. First, 5 U.S.C. § 7532 applies to all government employees regardless of whether they hold a clearance, while the executive order applies only to those already holding a clearance. Second, it allows for the immediate suspension without pay of the employee before any appeals procedures are provided. In contrast, under Executive Order 12968, the employee ordinarily would remain on the government payroll even though his access to classified information is suspended until his appeal rights under the executive order had been exhausted.[505] Third, upon loss of a security clearance under the executive order, if the agency has adopted regulations requiring such a reassignment, a government employee has the right to reassignment to another position not requiring a clearance.[506] Under Section 7532, an employee has no such right. Finally, if an employee's right to access is revoked under the executive order and his position requires a security clearance, and there are no agency regulations requiring reassignment, the employee would still have a right to appeal to the Merit Systems Protection Board if he was terminated, on the ground that the agency failed to follow procedural require-

ments in revoking the clearance.[507] Under 5 U.S.C. § 7532 the head of the agency taking the action may suspend an employee without pay when he considers it necessary in the interests of national security and may remove the suspended employee if he determines it to be necessary or advisable in the national interest.[508] The decision of the agency head is final with no further appeal.

After suspension, but before termination, an employee does have certain appeal rights under 5 U.S.C. § 7532. The employee must be notified of the reasons for the suspension but only to the extent that the agency head determines that it is in the interest of national security. Within 30 days after notification, the employee may submit statements or affidavits showing why he should be restored. For some employees that is the extent of their appeal rights. Only if an employee is a United States citizen, has completed his trial or probationary period, and has a permanent or indefinite appointment are there additional rights of appeal. In that case, the employee is entitled, after suspension and before removal, to a written statement of the charges against him as specific as security considerations permit and an opportunity to answer the charges and submit affidavits. The citizen-employee is also entitled to a hearing before an agency authority constituted for that purpose, a review of the case by the agency head or his designee before a final adverse decision, and a written statement of the decision of the head of the agency.[509] Although the nature of the hearing is not defined by the statute, it probably means a full trial-type hearing allowing for the presentation and cross-examination of witnesses.[510]

If a hearing is necessary, OPM has established procedures for the composition of agency security hearing boards.[511] OPM will obtain nominations for security hearing board members whose selection, after investigation, have been determined to be "clearly consistent with the interest of national security." Persons sitting as board members must be competent and disinterested government employees from outside the agency concerned. Personnel security officers and personnel investigators may not serve as board members because of the requirement that the board be disinterested.[512] When an agency wants to establish a security hearing board, it will request from OPM a list of names of approved persons from which to make its selection.[513]

A removal under Section 7532 permanently bars a person from employment by the agency from which he was removed. However, he may be restored to duty at that agency at the discretion of the agency head.[514] It does not automatically exclude him from employment by any other federal government agency, but if another agency seeks to employ that person, it must first consult with the Office of Personnel Management. It is OPM, and not the employing agency, that has the final authority to determine whether the person is eligible for further employment in another agency.[515]

Because of the stringent limitation on the use of Section 7532 and the availability of summary procedures under other statutes, executive orders or agency regulations, this statutory authority has fallen into disuse. Another reason for its disuse is that a summary dismissal also has the practical drawback of the government losing control of the person considered a security risk. If the person is deemed a security threat, but there is insufficient evidence for a criminal prosecution, agencies will often try avoiding putting an employee in a desperate position. To minimize any potential security breach and prevent the

suspected employee from fleeing or selling the information he has, the agency may keep the employee on the payroll but insulate that person from further contact with sensitive information until the classified information he does possess can be neutralized.

CHAPTER 16

Classified Information in Judicial Proceedings and the Classified Information Procedures Act

Criminal Prosecutions

The protection of national security information is of concern not only within the Executive Branch of the government and in industry, but also, at times, in court proceedings. It can be involved in both criminal cases, particularly those involving espionage, and in civil suits, for example, discrimination complaints by government employees working in intelligence agencies. The disclosure of classified information is of particular concern in criminal prosecutions because of the conflict of the interest of protecting government secrets with the right of defendants to be confronted with the evidence used against them. In this regard, Congress has enacted the Classified Information Procedures Act (CIPA) to protect classified information in criminal proceedings.[516]

The purpose of CIPA was to harmonize a defendant's right to obtain and use exculpatory material at trial, with the government's right to protect classified information in the nation's interest.[517] CIPA establishes procedures for permitting and protecting the use of classified information during a criminal trial, including the use of protective orders and sanctions. Sanctions vary and may be as severe as dismissal of an indictment if the government refuses to produce information that the court determines to be essential to the defense.[518]

The specific criminal trial procedures provided by the CIPA are beyond the scope of this review. However, of interest here are the personnel security procedures required by CIPA in such cases. Because of separation of powers concerns for the independence of the Judiciary, Section 9 of CIPA mandated that the Chief Justice of the United States, in consultation with the Attorney General, the Director of the CIA, and the Secretary of Defense, prescribe rules for the protection of unauthorized disclosure of classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Those rules were published in February 1981 and are found as a note to 18 U.S.C. App. 3, § 9.[519]

The security procedures established by the Chief Justice require that, in any criminal case where classified information is expected, a Court Security Officer shall be appointed who has a demonstrated competence in security matters.[520] The Court Security Officer must be recommended by the Attorney General and certified by the DOJ's Security Officer as cleared for the level and category of classified information involved. That person may come from the Executive Branch but is responsible to the court for information, physical, personnel, and communications security.

Any court personnel, i.e., persons appointed by the court or providing service to it requiring access to classified information, must first be cleared. A clearance is not required for justices and judges.[521] CIPA does not absolutely require that defense counsel

and other "persons associated with the defense," e.g., experts, secretaries, and law clerks, be cleared (although normally a background investigation is done on everyone). However, even if they will not submit to an investigation, the government may obtain information about their trustworthiness" by any lawful means," and may bring that information to the attention of the court for its consideration in framing appropriate protective orders.[522] While a defendant may select anyone for his defense team, if a person on the defense team is not considered sufficiently trustworthy to protect national security information, a protective order may prevent their having access to necessary information.

CIPA places juries on the same level of unquestioned trustworthiness as Justices of the Supreme Court. No investigation or security clearance is required of any member of the jury, nor may its functions, including access to classified information introduced as evidence, be interfered with.[523] While CIPA makes the jury sacrosanct, in reality the government can use its peremptory challenges or its challenges for cause to prevent the seating of any juror it considers untrustworthy.

The Court Security Officer is responsible for marking all court documents containing classified information with the appropriate level of classification and with any special access controls.[524] Every document filed by the defendant must be filed under seal and promptly turned over to the Court Security Officer who, in consultation with the government's attorney or an agency representative, determines whether it contains classified information. If it does contain classified information, the appropriate classification marking will be placed on the document and it will remain under seal.

DOJ Litigation Security Section

Court Security Officers in practice are provided by the Litigation Security Section, a unit within the DOJ Security and Emergency Planning staff, which is under the direct supervision of the DOJ Security Officer.[525] This section consists of five security specialists and their support staff whose primary function is to provide security to the federal courts under CIPA. It acts as advisor to the courts in criminal cases, creating security procedures and initiating personnel investigations, as required. It will also, on request of government attorneys, provide advice and assistance in criminal cases in state courts and in civil proceedings involving classified national security information.

The Court Security Officer will clear defense counsel and their staff, court personnel, court reporters, judges' assistants, court clerks, and other court personnel other than justices and judges, who are involved with classified information, using the same adjudicative and investigative standards that apply to all government personnel.[526] Each person needing access to classified information is required to fill out a SF 86, two fingerprint cards, an IRS tax waiver, and a DOJ credit information waiver form. The security investigation itself is conducted by the FBI.

Determinations of document classification are not made by the Court Security Officer. All documents that need to be classified or declassified are forwarded by the Court Security Officer to the originating agency for classification decisions.

Although the Litigation Security Section is a part of the DOJ and is located in the Main Justice Department Building in Washington, DC, it has no contact with DOJ personnel regarding litigation strategy. The section advises the courts only, creating a "wall" between it and the prosecuting attorneys to avoid any semblance of favoritism by the government. Once appointed by the court, it may also act as security advisor to defense counsel when requested. The section has, at times, provided secure facilities to defense attorneys in the courthouse itself or space in private buildings where no other security facilities were available.

The Litigation Security Section may get involved in state criminal cases, if requested by a federal government attorney, where classified information is involved. An example is a California court case in which the defendant was convicted of murder that had occurred on the premises of a contractor doing classified government work. During the sentencing phase, the defendant wanted to introduce information concerning a classified position he had previously held with an intelligence agency.

The pending workload of the Litigation Security Section at the time of this writing is 32 criminal cases and 21 civil cases. The section receives, on average, four to five new cases per year. Each of the five security specialists is designated as a Court Security Officer so that any of them can assist any court needing the Section's services.

Civil and Administrative Proceedings

Civil and administrative cases involving classified information are not covered by CIPA.[527] When those situations arise, at the request of the government's attorneys, the Litigation Security Section will notify the court and offer its assistance. Although courts are not obligated to accept, they generally do. The section will not respond to requests for assistance from private counsel until a Court Security Officer is appointed by the court in a particular case.

Access to classified information by participants in noncriminal proceedings is addressed in DOJ regulations.[528] Except for members of Congress, justices of the Supreme Court, and judges of United States district courts and courts of appeal, all other legislative and judicial personnel who require access to classified information must be determined to be eligible by the DOJ Security Officer under the Uniform Adjudicative Standards.[529]

Persons other than employees of the Executive Branch involved in litigation with the government who require access to classified information, classified either by DOJ or in its custody, must be investigated and cleared by DOJ. Employees of government contractors who have already been cleared by the Defense Security Service under the Industrial Security Program do not need further clearance unless a higher level of clearance is needed for the litigation.[530] Since all information connected to litigation with the federal government eventually come into the custody of the DOJ, its control over litigation security is comprehensive.

The standards for determining eligibility for access to classified information are the same for nongovernment personnel as for DOJ employees. DOJ regulations provide

that "no person" may be given access unless that person has been determined to be eligible under the standards of Executive Order 12968 (which applies to government employees or contractors), has a demonstrated need-to-know, and has signed an approved nondisclosure agreement.[531]

Civil litigation involving classified information can be in many contexts. Claims arising from classified government contracts is one area. Suits by government employees of agencies doing classified work such as the CIA or the FBI, who claim discrimination in the workplace are another. While the claim might involve an issue as mundane as a poor-performance evaluation, or failure to be selected for promotion, the location of the workplace or the names of the supervisors might be classified. Freedom of Information Act suits or denaturalization proceedings are other examples.[532] Although the government cannot forbid litigants from selecting attorneys of their choice, it can, if not satisfied with the trustworthiness of counsel, refuse to disclose classified information unless ordered by the court.

If classified information is involved in litigation before administrative agencies, such as the Equal Employment Opportunity Commission, clearances for administrative judges, attorneys, and support personnel are required. In those cases, since the agency involved, rather than DOJ, conducts the litigation, the investigations and clearances are provided by the litigating agency. The litigating agency will provide, as necessary, secure hearing rooms, cleared court reporters, and working and storage facilities for the litigant's counsel to prepare their case and to store classified information. Since the litigant's counsel does not normally have approved facilities for the storage of classified information, the agency will provide declassified or redacted copies of documents, including transcripts and documentary evidence for counsels' use in their offices. Where the names of the parties are classified, such as for covert employees of the CIA, cases will be filed under a pseudonym.

Before a clearance is granted, a standard Classified Information Secrecy Nondisclosure Agreement is required of counsel.[533] In conjunction with that agreement, a protective order will be entered requiring nongovernment counsel to submit pleadings to the Court Security Officer for review before filing. The time of that submission is considered the time of filing with the court. Certain agencies such as the CIA use their own form of Secrecy/Nondisclosure Agreement which, itself, requires that before the filing of any court pleading or other documents that may contain national security information, counsel must notify the agency granting the clearance "so that appropriate security protection can be sought." Where the proceedings are before an administrative agency, such as the EEOC, rather than in a court and where all parties have been previously cleared and where the hearing is held in secure facilities, it is not required that all submissions first be presented to the agency for declassification before being submitted to the hearing officer.

About the Author

Sheldon I. Cohen has been in the private practice of law in Washington, DC, and Arlington, VA, since 1964. He has handled government and private employment cases throughout that time, with emphasis on national security law for the last 20 years. Mr. Cohen was Chair of the American Bar Association, Administrative Law Section, Committee on National Security Interests, from 1990 through 1994. He was Chair of the American Bar Association (ABA), Administrative Law Section, Government Personnel Committee, from 1989 to 1993. He also served as Vice Chair of the ABA Committee on Contracting with National Security Requirements of the Public Contracts Law Section. As Chair and Vice Chair of those Committees, the author headed the ABA's efforts in defeating a proposed 1989 Presidential Executive Order that would have eliminated all appeal rights for government employees whose security clearances were threatened. He coordinated the ABA's involvement in the drafting of the *National Industrial Security Operating Manual*. The author also spearheaded the ABA's efforts to obtain additional appeal rights in employee security clearance cases which were included in Executive Order 12968 in 1995 and headed the ABA's participation in the drafting of the Uniform Adjudicative Guidelines issued by the Security Policy Board in 1997.

The author regularly practices before the Defense Office of Hearings and Appeals representing contractor employees and handles classified personnel matters before various government agencies.

Notes

1. *Halperin vs. CIA*, 629 F.2d 144, 154-162 (D.C. Cir. 1980).

2. U.S. Constitution, Art. II, §. 2. *Dept. of Navy v. Egan*, 484 U.S. 518, 527 (1988); *Totten v. United States*, 92 U.S. 105 (1876). See *United States v. Reynolds*, 345 U.S. 1 (1953); *Weinberger v. Catholic Action of Hawaii*, 454 U.S. 139 (1981).

3. A good historical review is found in Quist, *Security Classification of Information*, Vol 1, Chap. 2, (U.S. Department of Energy, 1989). It is posted on the Web site of the Federation of American Scientists, *www.fas.org/sgp/library/quist*.

4. E.O. 9835 (1947), as amended by E.O. 10237 (1951).

5. E.O. 11652 (1972); E.O. 12065 (1978); E.O. 12356 (1982) and E.O. 12958 (1995).

6. Compare Executive Orders 12065 and 12958 with Executive Orders 11652 and 12356.

7. E.O. 10450 (1953).

8. E.O. 10865 (1960).

9. 40 Stat. 217, as amended.

10. 61 Stat. 496 (50 U.S.C. 401-432).

11. 68 Stat. 919 (42 U.S.C. 2161-2169).

12. 108 Stat. 3435 (50 U.S.C. 801).

13. 5 U.S.C. 552.

14. 50 U.S.C. 403(d)(3). This authority is further implemented by Executive Order 12. 333 §1.5(h).

15. See *Report of the Commission on Protecting and Reducing Government Secrecy*, pp. 23-24 (Government Printing Office, 1997) (hereinafter referred to as the *Secrecy Commission Report*). Information protected under the Atomic Energy Act is termed "Restricted Data (RD)" and when used in connection with military use of atomic weapons is referred to as "Formerly Restricted Data (FRD)."

16. 108 Stat. 3435 (50 U.S.C. 801).

17. E.O. 12958, § 1-1.

18. Id., § 1.3.

19. Id., §§ 4.1(h), 4.4.

20. 10 U.S.C. 119(e)(2). See *Secrecy Commission Report*, p. 26 (1997).

21. 61 Stat. 496 (50 U.S.C. 401 et seq); E.O. 12333, 46 Fed. Reg. 59941, Dec. 4, 1961.

22. E.O. 12958, § 4.2.

23. Id., § 4.4.

24. E.O. 12968, § 3.1.

25. The Security Policy Board is the Board established by the President to consider, coordinate, and recommend policy directive for the U.S. security policies, procedures, and practices. It was established by Presidential Decision Directive/NSC-29, (PDD-29) (Sept. 16, 1994), and is referred as the cognizant authority for issuing the uniform standards in E.O. 12968 §1.1(j).

26. See DoD Directive 5200.2-R. Appendix I.

27. DCID 6/4.

28. The National Industrial Security Program, A Report to the President by the Secretary of Defense, p. 21, November 1990 (hereinafter cited as the Industrial Security Program Report), Secrecy Commission Report, p. 10.

29. A comprehensive discussion of the earlier case law is found in: Haag and Denk, *Due Process in Matters of Clearance Denial and Revocation* (Defense Personnel Security Research and Education Center, 1988)(PERS-TR-88-004).

30. See *Cafeteria and Restaurant Workers Union v. McElroy*, 367 U.S. 886 (1961).

31. "Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment and to decide whether the agency should have been able to make the necessary affirmative prediction with confidence. Nor can such a body determine what constitutes an acceptable margin of error in assessing the potential risk" [quoting *Dept of Navy v. Egan*, 484 U.S. 529]. . . These decisions are based on grounds of institutional competence, separation of powers and deference to the Executive on national security matters. *Stehney v. Perry,* 101 F.3d 925, 931-32 (3rd. Cir. 1996).

32. *Webster v. Doe*, 486 U.S. 592, 603 (1988).

33. Ibid.

34. In an undated (circa 1997) "Discussion Paper" of a "working group" in the Department of Justice, the arguments for and against judicial review of

discrimination claims in security clearance cases were reviewed. The group concluded that *Webster v. Doe* appeared to require judicial review of equitable constitutional claims, but agreed that any remedy should not permit a court to order the Executive Branch to grant a security clearance. The discussion paper, *Judicial Review of discrimination in Security Clearance Decisions,* is available on the Internet wet site of the Federation of Government Scientists, Government Secrecy Project: *www.fas.org/spg.*

35. See, *Able v. United States*, 155 F.3d 628 (2nd Cir. 1998); *Jackson v. Air Force* (unpublished) 1997 W.L. 759144 (9th Cir. 1997); *Holmes v. California Army National Guard,* 124 F.3d 1126 (9th Cir.1997).

36. E.O. 12968, § 3.1(c).

37. Compare *Greene v. McElroy,* 360 U.S. 474, 496 (1959) with *Vitarelli v. Seaton*, 359 U.S. 535 (1951) and *Dept. Of Navy v. Egan,* 484 U.S. 518 (1988).

38. 360 U.S. 496 (1959).

39. 484 U.S. 528.

40. E.O. 12968, § 5.2.

41. E.O. 12968, §. 5.1.

42. *Industrial Security Program Report.*

43. *Industrial Security Program Report*, pp. 8-9.

44. National Security Directive 63 remains classified, but there is an unclassified "Fact Sheet" summarizing the Directive's requirements which is discussed in Chapter 3.

45. *DoD Report on Personnel Security, FY 1993*, p. 9 (Defense Personnel Security Research Center).

46. See GAO Report, Background Investigations, Impediments to Consolidating Investigations and Adjudicative Functions, Mar. 1995, (GAO/NSIAD-95-101).

47. The NISPOM is now designated as DoD Manual 5220.22-M.

48. Counterintelligence and Security Enhancements Act, P.L. 103-359, § 801, 108 Stat. 3434, Oct. 14, 1994 (50 U.S.C. 435).

49. H.R. Conf. Rep. No. 103-753, 103rd Cong. 2d. Sess., Sept. 27, 1994.

50. E.O. 12968, Sec. 3.2(b). The Security Policy Board was created by Presidential Decision Directive 29. A "Fact Sheet" describing the contents of that Directive is found at the Security Policy Board Web site: *www.spb.gov.*

51. 63 Fed. Reg. 4572, Jan. 30. 1998, 32 C.F.R. Part 147.

52. The Department of Defense has included the uniform standards in DoD 5200.2-R. Appendices I and N. The Central Intelligence Agency has incorporated them in DCID 6/4, Annexes A and C.

53. The Commission was created by P.L. 103-236, Title IX, 108 Stat. 525, Apr. 30, 1994 (50 U.S.C. 435, note).

54. S. 712, 105th Cong. 2d sess.

55. Hearings were held on Mar. 25, 1997 and May 7 1998 by the Senate Committee on Governmental Affairs. They are available on the Web site of the Federation of American Scientists, *www.fas.org/spg/congress.* The Committee issued its report, S. Rep. 105-258, 105th Cong., 2d Sess. on Jul. 22, 1998.

56. S. 22, 106th Cong. 1st. Sess.

57. National Security Directive 63 may be found at the Federation of American Scientists Web site: *www.fas.org/spg/othergov.*

58. Counterintelligence and Security Enhancements Act of 1994, P.L. 103-359, Sec. 801(a)(2), Oct. 14, 1994; (50 U.S.C. 435).

59. E.O. 12968, § 3.2(b).

60. 63 Fed. Reg. 4572, Jan. 30, 1988; 32 C.F.R. Part 147, Subpart B. The Uniform Guidelines and Standards are issued as part of the DoD regulations as that Department has the administrative responsibility for supporting the Security Policy Board.

61. 32 C.F.R. § 147.18.

62. E.O. 12958, § 4.4, 60 Fed. Reg. 19825 (Apr. 20, 1995).

63. "Q" and "L" designations used by the Department of Energy under the Atomic Energy Act are technically known as "accesses," but for the sake of simplicity in this book are here referred also as clearances. "Q" is the equivalent to Top Secret and "L" is the equivalent to Confidential.

64. 32 C.F.R. § 147.19.

65. 32 C.F.R. § 147.24.

66. See, DoD 5200.2-R, §§ 1-312,1-313, 2-302; Chap. II, Sec. 2; Chap. III, App B.

67. 32 C.F.R. Part 147, Subpart B, Attachment A.

68. 32 C.F.R. Part 147.

69. Ibid.

70. 32 C.F.R. Part 147, Subpart B, Attachment A.

71. 32 C.F.R. Part 147, Subpart B, Attachment B.

72. 32 C.F.R. Part 147, Subpart B, Attachment C.

73. E.O. 12968, § 3.3.

74. 32 C.F.R. § 147.29.

75. 32 C.F.R. Subpart C.

76. DoD Directive 5200.2-R, App. G, Para. B.

77. Ibid.

78. Id., Para. D.3.

79. See Chapter 5.

80. E.O. 10450, § 3(b).

81. OPM regulations on national security investigations are found at 5 C.F.R. Parts 732 and 736. They mention only the lower three sensitivity levels, but refer to the *Federal Personnel Manual*, Chapter 732, which defines all four sensitivity levels and prescribes the investigative requirements for each. The FPM was officially abolished in 1993 but the procedures described in it are still followed by OPM. 5 C.F.R. Parts 731, 732 and 736 are currently under revision because they were adopted prior to Executive Order 12968 and do not incorporate its new standards and procedures. Proposed revisions to Part 731 were published on Jan. 28, 1999. 64 Fed. Reg. 4336-4342. Proposed revisions to Parts 732 and 736 were last published on Jan. 5, 1996. 61.Fed.Reg. 384-402. The investigative requirements formerly found in the FPM are also expected to be incorporated in the new regulations (see Chapter 4).

82. F.P.M. Chap. 732, Subchap. 2.

83. See Chapter 4.

84. The Defense Security Service now also includes the DoD Polygraph Institute (DODPI). The former DoD Security Institute (DoDSI) was disestablished in Sept. 1998, and its functions have been assumed by the DSS Academy. The DSS Charter is DoD Directive 5105.42.

85. DoD Directive 5200.2. The DoD Personnel Security Program is detailed in DoD 5200.2-R, codified at 32 CFR 154.

86. DoD Directive 5220.22. *The National Industrial Security Program Operating Manual* ("NISPOM") is DoD 5220.22-R.

87. The organization of DSS is described on its Web site, *www.dss.mil.* Unless otherwise referenced, information concerning DSS was provided during an interview with representatives of DSS's Office of General Counsel and of its investigative branches.

88. DoD Directive 5200.2-R, Par. 2-401.

89. DoD Directive 5200.2-R, Par. 2-402.

90. Ibid.

91. Information provided during an interview with the Office of the Associate Director, OPM Investigations Service.

92. OPM Investigations Service uses USIS, Inc., which is made up of former OPM investigators. NRO uses a private organization, USIS, Inc., to do its investigations. OMNISEC, an organization comprised of retired CIA agents, does some investigations for the CIA. The FBI also uses a group of former and retired FBI agents that it calls the Background Investigations Contract Service (BICS).

93. DoD Directive 5200.2-R, Par. 2-400; DoD Directive 5100.2-3, *Administrative Arrangements for the National Security Agency*, May 17, 1967.

94. DoD Directive 5220.6; Par. B.3.

95. DSS Manual 20-1-M is designated "For Official Use Only." It is probably similar in content to the OPM investigator's handbook, *Conducting and Reporting Personnel Investigations*, FPM Supplement 736-71.

96. DoD Directive 5200.2-R, Par. 2-205.

97. DSS has a form for requesting an individual's file that is available on its Web site at *www.dss.mil.*

98. There are seven CAF's: Army, Navy, Air Force, Joint Staff, Washington Headquarters Services, Defense Intelligence Agency, and National Security

Agency. See Audit Report of the DoD Inspector General, No 97-196, *Personnel Security in the Department of Defense*, Jul. 25, 1997.

99. NISPOM, Par. 2-100.

100. Overseas personnel investigations are conducted by the appropriate military department investigative organization under the direction and control of DSS. DoD 5200.2-R, Par. 2-404.

101. OPM conducts 40 percent of federal personnel security investigations, the Defense Security Service conducts 40 percent, the FBI and the NSA do about 10 percent, and other agencies do the remaining 10 percent. Unless otherwise indicated, information concerning the operations of the OPM Investigations Service was provided by the OPM Office of the Associate Director for Investigations.

102. OPM does approximately 345,000 investigations a year, of which 45,000 are national security investigations. Many of the nonsecurity investigations are done to a level suitable for a national security investigation, due to the sensitivity of the position for which the individual is being considered.

103. OPM Federal Investigations Notice, Letter No. 99-08, Aug. 12, 1999.

104. OPM does adjudicate "suitability" determinations for all agencies for which it does such investigations.

105. OPM investigator's handbook, FPM Supplement 736-1, *Conducting and Reporting Personnel Investigations*, Appendix C (Feb. 1999).

106. Data on the results of OPM's investigations for Fiscal Years 1996 through 1998 was supplied by the OPM Investigations Service.

107. The difference between the data cited and 100 percent reflects "other issues" raised during the investigation.

108. Regulations covering suitability determinations are found at 5 C.F.R. Part 731. The latest proposed revision to this Part was published at 64 Fed. Reg. 4336, Jan.28, 1999.

109. 5 C.F.R. §732.201(c).

110. Proposed revisions to 5 C.F.R. Parts 732 and 736 were published on Jan. 5, 1996 at 61 Fed. Reg. 394. They are still under consideration by OPM as noted at 64 Fed. Reg. 4336, Jan. 28, 1999.

111. Compare 5 C.F.R. § 736.103 with proposed § 736.201, 61. Fed. Reg 401.

112. Proposed § 736.203, 61 Fed. Reg. 401.

113. Ibid. See investigator's handbook, Subchap. I.B.

114. Proposed § 736.203.

115. DoD Directive 5220.6.

116. *Secrecy Commission Report*, pp. 11-12, Government Printing Office, 1997.

117. Counterintelligence and Security Enhancements Act of 1994, P.L. 103-359, Sec. 801(a)(2), Oct. 14, 1994 (50 U.S.C. 435).

118. E.O. 12968, Sec. 3.2(b). The Security Policy Board was created by Presidential Decision Directive 29. A "Fact Sheet" describing the contents of that Directive is found at the Security Policy Board Web site: *www.spb.gov.*

119. 63 Fed. Reg. 4572, Jan. 30, 1988; 32 C.F.R. Part 147, Subpart B. These guidelines were issued as part of the DoD regulations because that Department has the responsibility for administratively supporting the Security Policy Board.

120. 32 C.F.R. § 147.18.

121. E.O. 12968 §§ 3.1(f), 3.2(b) authorizes varying standards for differing levels of access, including those for special access programs. The Security Policy Board's guidelines further address these special requirements. 32 C.F.R. § 147.19(a). Special access programs are authorized by E.O. 12958, Sec. 4.4, 60 Fed. Reg. 19825 (Apr. 20, 1995).

122. 32 C.F.R. § 147.23.

123. Security Procedures Established Pursuant to P.L. 96-456. 18 U.S.C. App. 3, § 9, note. (Oct. 15, 1980). See Chapter 17.

124. 32 C.F.R. § 147.1.

125. 32 C.F.R. §§ 147.3-147.15.

126. 32 C.F.R. § 147.2.

127. Ibid.

128. Ibid.

129. The only reported decisions are those of the Defense Office of Hearings and Appeals (DOHA) affecting contractor employees as part of the Industrial Security Program (see Chapter 7, and those of the Department of Energy Office of Hearings and Appeals (see Chapter 13). DOHA decisions beginning in 1996 are

available at *www.defenselink.mil/dodg/doha*. Representative DOHA cases are cited in this chapter. The cases are fact-intensive and are legion. Prior to 1996 DOHA was known as the Defense Industrial Security Review Board (DISCR). For convenience, all earlier DISCR cases are here referred to as DOHA cases.

Department of Energy decisions are available at *www.oha.doe.gov/persec2.htw*. Decisions of the military departments central adjudication facilities or any department Personnel Security Appeals Board affecting military personnel or government employees are not reported.

130. DOHA Case No. 98-0056, June 19, 1998 (clearance granted); DOHA Case No. 96-0649, Apr. 22, 1997 (clearance granted).

131. DOHA Case No. 97-0233, Aug. 11, 1997 (clearance granted).

132. 32 C.F.R. § 147.3.

133. There have been only two reported decisions of the Defense Office of Hearings and Appeals under this guideline and its predecessors since 1972. DISCR OSD Case No. 82-0130, Dec. 13, 1982, aff'd July 22, 1983 (clearance granted); DISCR OSD Case No. 88-1198, Feb. 18, 1992 (clearance denied on other grounds). Seven cases were brought between 1966 and 1969, four of them denying clearance and three granting: OSD Case No. 66-488, Apr. 19, 1968; OSD Case No. 66-580, Sept. 4, 1968; OSD Case No. 68-238, May 13, 1969; OSD Case No. 68-726, Dec. 17, 1969; OSD Case No. 68-254, Mar. 10, 1970; OSD Case No. 68-522N, Apr. 28, 1971; OSD Case No. 69-29, Mar. 23, 1970.

134. DoD Directive 5200.2-R, Par. 2-401. See Chapter 4.

135. 32 C.F.R. § 147.4.

136. DOHA Case No. 97-0699, June 25, 1998 (clearance denied).

137. 32 C.F.R. § 147.5.

138. DOHA Case No. 98-0254, Oct. 19, 1998 (clearance denied).

139. DOHA Case No. 98-0313, Sept. 16, 1998 (clearance granted); DOHA Case No. 97-0356, Dec. 21, 1997 (clearance denied).

140. 32 C.F.R. § 147.6.

141. DOHA Case No. 98-0113, Sept. 18, 1998 (clearance denied).

142. DOHA Case No. 96-0641, Aug. 12, 1997 (clearance denied).

143. DOHA Case No. 97-0618, Mar. 31, 1998 (clearance denied); DOHA Case No. 98-0077, Jun. 25, 1998 (clearance granted).

144. DOHA Case No. 98-0247, July 30, 1998 (clearance granted).

145. DOHA Case No. 97-0605, July 8, 1998 (clearance denied).

146. DOHA Case No. 97-0737, Apr. 21, 1998 (clearance granted); DOHA Case No. 97-0465, Jan. 23, 1998 (clearance granted).

147. See, *Able v. United States*, 155 F.3d 628 (2d Cir. 1998); *Jackson v. Air Force* (unpublished) 1997 W.L. 759144 (9th Cir. 1997); *Holmes v. California Army National Guard,* 124 F.3d 1126 (9th Cir.1997).

148. 32 C.F.R. § 147.7.

149. DOHA Case No. 98-0269, Oct. 14, 1998 (clearance denied); DOHA Case No. 98-0202, Oct. 14, 1998.

150. DOHA Case No. 97-0457, Jun. 4, 1998 (clearance denied).

151. DOHA Case No. 98-0370, Oct. 2, 1998 (clearance denied); DOHA Case No. 98-0303, Sept. 23, 1998 (clearance denied); and DOHA Case No. 97-0830, June 6, 1998 (clearance denied).

152. 32 C.F.R. § 147.8.

153. DOHA Case No. 98-0317, Sept. 11, 1998 (clearance granted).

154. DOHA Case No. 97-0783, Apr. 14, 1998 (clearance denied).

155. DOHA Case No. 98-0368, Sept. 3, 1998 (clearance granted); DOHA Case No. 98-0358, Sept. 16, 1998 (clearance denied).

156. 32 C.F.R. § 147.9.

157. The Department of Energy reports for Fiscal Years 1995 through 1997 that of 312 denials and revocations, 63 percent involved alcohol or drug abuse. (See Chapter 13.) DOHA decisions for 1996 through 1998, show of a total of 603 cases, 485 of them involved financial considerations, drugs, alcohol, or a combination of them.

158. DOHA Case No. 98-0380, Oct. 13, 1998 (clearance granted).

159. DOHA Case No. 98-0266, Sept. 11, 1998 (clearance granted).

160. 32 C.F.R. § 147.10.

161. The FBI still follows the former practice of having very specific and detailed regulations on the type, period of use and amount of substance used. See Chapter 14.

162. DOHA Case No. 98-0091, Jul. 6, 1998 (clearance granted); DOHA Case No. 98-0066, Sept. 11, 1998 (clearance denied).

163. DOHA Case No. 98-0364, Sept. 25, 1998.

164. DOHA Case No. 98-0405, Oct. 22, 1998 (clearance denied).

165. DOHA Case No. 98-0303, Sept. 23, 1998 (clearance denied).

166. Both civilian employees and military members may be dismissed for drug use even if there is no security clearance involved under applicable personnel regulations.

167. 32 C.F.R. § 147.11.

168. E.O. 12968, § 3.1(e), 60 Fed. Reg. 40250, Aug. 7, 1995.

169. 32 C.F.R. § 147.12.

170. DOHA Case No. 97-0798, Mar. 19, 1998 (clearance denied).

171. DOHA Case No.97-0676, Apr. 6, 1998.

172. DOHA Case No. 98-0247, Jul. 30, 1998 (clearance granted); DOHA Case No. 97-0184, Aug. 17, 1998 (clearance granted).

173. DOHA Case No. 98-0329, Sept. 2, 1998 (clearance denied).

174. DOHA Case No. 97-0419, Jan. 27, 1998 (clearance granted).

175. 32 C.F.R. § 147.13.

176. DOHA Case No. 97-0435, Jul. 14, 1998 (clearance denied).

177. Prosecution for disclosure of classified information is provided by 18 U.S.C. §§ 793, 798. See, DOHA Case No. 97-0087, Aug. 21, 1997 (clearance denied); DOHA Case No. 97-0061, Jul. 1, 1997 (clearance denied).

178. DOHA Case No. 97-0435, Feb. 27, 1998 (clearance granted).

179. DOHA Case No. 96-0605, Jul. 23, 1997 (clearance denied); DOHA Case No. 93-1234, Jan. 20, 1995 (clearance denied).

180. 32 C.F.R. § 147.14.

181. There were no DOHA decisions applying Guideline L for 1996 through 1998.

182. 32 C.F.R. § 147.15.

183. DOHA Case No. 96-0687, Apr. 10, 1997 (copying of commercial software programs while in college) (clearance denied).

184. DOE Case No. USO-0122, 26 DOE ¶ 82,777, May 2, 1997.

185. 484 U.S. 518 (1988).

186. The Navy regulation is OPNAV.INST 5510.30A (Mar.10, 1999); the Army regulation is AR 380-67 (Sept. 9, 1988, as amended by change 3); and the Air Force regulation is AFINST 31-501 (May 2, 1994, as revised, Apr. 22, 1996). The Office of the Joint Chiefs of Staff does not have its own regulation.

187. 484 U.S. at 528.

188. The history of E.O. 12968 is discussed at length in a collection of papers prepared for an American Bar Association Seminar: *Security Clearance Practices: Balancing the Interests of the Government and the Individual* (Sept. 19, 1990).

189. Keeping the Nations Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices (1985) (The Stilwell Commission). The report is posted on the Web site of the Federation of American Scientists, www.fas.org/sgp/library.

190. P.L. 103-359, Title VIII, 108 Stat. 3434, Oct. 14, 1994 (50 U.S.C. 435).

191. See Statement by the White House Press Secretary accompanying the release of E.O. 12968, Aug. 4, 1995. The Adjudicative Guidelines may be found on the Security Policy Board Web site: *www.spb.gov.*

192. E.O. 12968, Secs. 1.1(b), 1.1(e), and 3.1(c).

193. Id., at Part 5, "Review of Access Determinations."

194. E.O. 12968. Sec. 2.2(b).

195. Ibid.

196. 360 U.S. 474, 508 (1959).

197. DoD 5200.2-R covers, in addition to access to classified national security information, assignment to "sensitive positions" even though such positions do not deal with classified information. A sensitive position is one in which the occupant could have "a materially adverse effect on the national security." All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive. See DoD Directive 5200.2-R, Secs. 1-321, 3-101 and Appendix K (ADP Position categories).

198. DoD Directive 5200.2-R, Secs. 6-100, 6-102.

199. Id., at Sec. 6-101(b)(2).

200. See footnote 186.

201. Id., at Sec. 6-102.

202. Id., at Sec. 6-102.

203. Id., at Sec. 8-102.

204. Id., at Sec. 8-200.

205. Id., at Sec. 8-201.

206. Id., at Sec. 8-201(d).

207. Id., at Appendix M.

208. The structure and functioning of the PSABs is described in Appendix M to DoD Directive 5200.2-R.

209. The structure and functioning of the personal appearance before DOHA is described in Appendix N to DoD Directive 5200.2-R.

210. Interview with the Office of DOHA's Chief Administrative Judge.

211. Statistical results of DOHA personal appearances were provided by the Office of DOHA's Chief Administrative Judge.

212. DoD Directive 5200.2-R, Sec. 8-201(d); Appendix M.

213. Statistical results of DOHA personal appearances were provided by the Office of DOHA's Chief Administrative Judge.

214. DoD Directive 5200.2-R, Appendix M, Para. 8.

215. Interview with the Office of DOHA's Chief Administrative Judge.

216. 360 U.S. 474, 507 (1959).

217. DoD Directive 5220.6 applies to the Office of the Secretary of Defense, the military departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Inspector General of the Department of Defense and the Defense agencies. By mutual agreement, it also extends to the: (a) Department of Agriculture, (b) Department of Commerce, (c) Department of Interior, (d) Department of Justice, (e) Department of Labor, (f) Department of State, (g) Department of Transportation, (h) Department of Treasury, (i) Environmental Protection Agency, (j) Federal Emergency Management Agency, (k) Federal Reserve

System, (l) General Accounting Office, (m) General Services Administration, (n) National Aeronautics and Space Administration, (o) National Science Foundation, (p) Small Business Administration, (q) United States Arms Control and Disarmament Agency, (r) United States Information Agency, (s) United States International Trade Commission, and (t) United States Trade Representative. (Part B.2).

218. DoD Directive 5220.6, Part B.6.

219. 360 U.S. 474, 508.

220. A detailed discussion of the organization and operations of DOHA, formerly known as the Directorate for Industrial Security Clearance Review (DISCR), is found in a collection of papers prepared for an American Bar Association Seminar, "Security Clearance Practices: Balancing the Interests of the Government and the Individual" (Sept. 19, 1990).

221. 32 C.F.R., Part 147, 63 Fed. Reg. 4572 (Jan. 30, 1998).

222. The three enclosures to DoD Directive 5220.6 are E.O. 10865, the Adjudicative Guidelines for determining eligibility for a clearance and an Additional Procedural Guidance for proceedings before DOHA (hereafter referred to as DOHA Additional Procedural Guidance). (The Additional Procedural Guidance is found at Appendix D).

223. An example of a Statement of Reasons and an Answer to the Statement of Reasons are included as Appendix F.

224. The adjudicative criteria were first formulated in 1953 in E.O. 10450, "Security Requirements for government Employees." The most recent formulation is the Uniform Adjudicative Guidelines restated in the DOD Personnel Security Regulation, 5200.2-R, Appendix I. (Included as Appendix B). Those guidelines are included in DoD Directive 5220.6 provided with the SOR.

225. DOHA Case No. 97-0403, May 13, 1998 (Clearance denied).

226. DOHA Additional Procedural Guidance, Para. 7.

227. Id., Para. 11.

228. There are no DOHA Appeal Board decisions on this point.

229. DOHA Additional Procedural Guidance, Para. 11.

230. Id., Para. 13.

231. In addition to the DOHA "Additional Procedural Guidance," the parties are provided a memorandum entitled: "Prehearing Guidance for DOHA Hearings," signed by the Chief Administrative Judge specifying, in detail, the conduct of the hearing (Appendix E).

232. *Department Of Navy v. Egan,* 484 U.S. 518, 531 (1988). E.g., DISCR OSD No. 89-1607 (Jul. 18, 1989).

233. DoD. Dir. 5220.6, Para. F.3.

234. DoD Dir. 5220.6, Enclosure 2.

235. DOHA Case No. 96-0785 (Sept. 3, 1998).

236. DOHA Case No. 97-0727 (Aug. 3, 1998); DOHA Case No. 97-0202 (Jan. 20, 1998).

237. DOHA Additional Procedural Guidance, Para. 22.

238. Interview with the Office of the Chief Administrative Judge.

239. Ibid.

240. DOHA Additional Procedural Guidance, Para. 42-46.

241. Id., Para. 44.

242. DOHA Case No. 97-0630 (May 28, 1998); DOHA Case No. 96-0152 (Jan. 14, 1997); DOHA Case No. 96-0228 (Apr. 3, 1997).

243. DOHA Additional Proecural Guidance, Para. 28.

244. Id., Para. 30.

245. Id., Para. 32.

246. Ibid.

247. E.g., *Stehney v Perry*, 101 F.3d 925 (3d Cir. 1996); *Brazil v Department of Navy*, 66 F.3d 193, 197 (9th Cir. 1995); cert. denied 517 U.S. 1103 (1996); *Dorfmont v Brown*, 913F.2d 1399 (9th Cir. 1990).

248. DOHA Additional Procedural Guidance, Para. 37-41.

249. Interview with the Office of the Chief Administrative Judge, Defense Office of Hearings and Appeals.

250. The requirement of the Administrative Procedures Act, 5 U.S.C. 552(a)(2), for public availability of agency opinions, technically had been met by having the opinions available in its headquarters' library. There had not been a realistic publication to DOHA's nationwide audience until the recent posting of decisions on the Internet.

251. 523 U.S. 303, 118 S.Ct. 1261, 1264-1266, 140 L.Ed 2d 413 (1998).

252. Id., 118 S.Ct. 1269. (Concurring Op.)

253. Id., 118 S.Ct. 1266.

254. Id., 118 S.Ct. 1272, f.n. 7. (Dissenting Op.)

255. *South Dakota v. Neville*, 459 U.S. 553, (1983); *Schmerber v. California*; 384 U.S. 757, 764 (1966).

256. *Secrecy Commission Report, 90.*

257. *Secrecy Commission Report, 90.* The Secrecy Commission Report cites: House Permanent Select Committee on Intelligence, Report on United States Counterintelligence and Security Concerns (1986); Office of Technology Assessment, Scientific Validity of Polygraph Testing: A Research Review and Evaluation--A Technical Memorandum, OTA-TM-H-15 (Washington, D.C.: Office of Technology Assessment, November 1983); House Permanent Select Committee on Intelligence, United States Counterintelligence and Security Concerns; and Department of Defense Polygraph Institute, Study of the Accuracy of Security Screening Polygraph Examinations.

    For additional information and examples of studies finding the polygraph to be scientifically valid in certain applications, see Department of Defense Polygraph Institute, *Bootstrap Decisions Making for Polygraph Examinations*, Final Report of DOD/PERSEREC Grant No. N00014-92-J-1795 prepared by Charles R. Honts and Mary K. Devout (Grand Forks: University of North Dakota, 25\4 August 1992); Charles R. Honts, *Theory Development and Psycho-physiological Credibility Assessment* (Boise State University, 1996); Charles R. Honts, 1994 *Final Report: Field Validity Study of the Canadian Police College Polygraph Technique*, Science Branch: Supply and Services Canada, contract #M9010-3-2219/01ST (Grand Forks: C. Honts Consultations, 1994); Christopher J. Patrick and William G. Iscono, *Validity and Reliability of the Control Questions Polygraph Test: A Scientific Investigation*, SBR Abstracts, Psychophysiology 24, No. 5 (September 1987): 604-5.

258. Gordon Barland, Charles R. Honts, and Steven Barger, *Studies of the Accuracy of Security Screening Polygraph Examinations* (Fort McClellan: Department of Defense Polygraph Institute, 24 March 1989), iii. The Secrecy Commission Report at p. 90, notes, however, that the DoDPI study was conducted in a

controlled setting and may not accurately reflect the conditions under which a polygraph is normally taken.

259. 118 S. Ct., 1265, f.n.6., 118 S. Ct. 1276 (Dissenting Op).

260. The concurrence of President Johnson was expressed in a "Memorandum to the Heads of Departments and Agencies" which prohibited the use of the polygraph in the Executive Branch except: (a) by Departments or Agencies having an intelligence or counterintelligence mission directly affecting national security, the use of which required the approval of the Chairman of the Civil Service Commission (now OPM); (b) for use for criminal investigations which required the approval of the Attorney General; and (c) in research and development which required the approval of either OPM or the Attorney General depending on the purpose. The memorandum explicitly limited conditions for its use and the rights to be afforded a person being polygraphed. The details the memorandum are essentially restated in the *Federal Personnel Manual* (FPM), Chap. 736, § 2-6. They have also been restated in proposed revisions to 5 C.F.R. Part 736, OPM's regulations on personnel investigations. See, proposed § 736.203 at 61 Fed. Reg. 394, 396, 401 (Jan. 5, 1996). Although the FPM was abolished on December 31, 1993, it will remain a useful source of current law and procedure until the proposed revisions are adopted. See, 64 Fed. Reg. 4336 (Jan. 28, 1999).

261. NSDD-84, approved by President Reagan on March 11, 1983.

262. FPM, Chap. 736, § 2-6.

263. NSA's use of the polygraph for employment screening was approved in *Stehney v. Perry*, 101 F.3d 925 (3d Cir. 1996).

264. Secrecy Commission Report, 90.

265. DoD Directive 5210.48, Para. D.7, D.8.

266. A Special Access Program is defined as: "a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." E.O. 12958, § 4.1(h) (1995).

267. DoD Directive 5210.48, Para. D.12(f).

268. DoD Directive 5210.48, Para. D.6, D.9 and G.1.

269. DoD Directive 5210.48, Para. D.12.

270. DoD Directive 5210.48, Para. D.1 to D.4.

271. DoD Directive 5210.48, Para. D.4.

272. Executive Order 12968, § 5.2(a)(2) requires disclosure of the investigative file but only to the extent that the documents would be provided under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (5 U.S.C.552a). Polygraph records as a class have been exempted by the CIA from disclosure under the Privacy Act. 32 C.F.R. §§ 1901.61(a), 1901.62(a)(1). The CIA's denial of polygraph records has been upheld by two Federal Courts of Appeal. *Blazy v. Tenet*, 1997 WL 315583 (D.C. Cir. 1998) aff'g, *Blazy v. Tenet*, 979 F. Supp. 10 (D.D.C. 1997); *Villaneuva v. Dept of Justice*, 782 F. 2d 528 (5th cir. 1986).

273. DOE Polygraph Examination Regulation, 10 C.F.R. Part 709 (64 Fed. Reg. 70961-70980, December 17, 1999.

274. *The Washington Post*, page A-8, Jul. 16, 2000.

275. DOHA ISCR Case. No. 94-1057 (Aug. 11, 1995).

276. Ibid. DoD Regulation 5210.48-R, Chap. 1 Para. C.D.1, however, provides that the "results of an analysis of the polygraph charts may be considered to have probative value in administrative determinations."

277. DOHA ISCR Case No. 96-0785 (Initial Decision) (Apr. 16, 1998).

278. DOHA ISCR Case No. 96-0785 (Appeal Board Decision) (Sept. 3, 1998).

279. DOHA ISCR Case No. 96-0785 (Remand Decision of the Administrative Judge) (Jan. 11, 1999).

280. DOHA ISCR Case No. 96-0785, Jun. 1, 1999.

281. *Hillen v. Department of the Army*, 35 MSPR 453 (987).

282. *Meier v. Department of Interior*, 3 MSPR 247 (1980).

283. *Woodward v. Office of Personnel Management*, 74 MSPR 389 (1997).

284. Compare cases favoring the government: *Roberts v. Department of the Treasury*, 8 MSPR 764 (1981); *Flores v. Department of Labor*, 13 MSPR 281 (1982); *Washington v. Department of Navy*, 21 MSPR 370 (1984); *Friedrick v. Department of Justice*, 52 MSPR 126, aff'd Fed. Cir. No. 92-3219(10/07/92);91); with cases favoring the employee: *Perez v. Department of the Navy*, 4 MSPR 52 (1981); *Williams v. Department of HUD*, 23 MSPR 213 (1984); *Moen v. Federal Aviation Administration*, 28 MSPR 556 (1985); *Ballew v. Department of the Army*, 36 MSPR 400 (1988); *Robancho v. Department of the Navy*, 52 MSPR 425 (1992).

285. *Kumferman v. Department of the Navy*, 785 F.2d 286 (Fed Cir. 1986).

286. Executive Order 10450, Sec. 9, Apr. 27, 1953.

287. DoD Directive 5200.2-R, Par. 12-100.

288. 32 C.F.R. § 147.24. See Chapter 2 for a further discussion.

289. Reference to the SII is found in the Chapters 732 and 736 *Federal Personnel Manual* (FPM) which was abolished in 1993.

290. F.P.M., Chap. 732, § 7-4.a.

291. F.P.M., Chap. 732, § 7-4.c.

292. F.P.M. Chap. 732, § 7-7.

293. F.P.M. Chap. 736, § 2-2.d.

294. DoD Directive 5200.2-R, Par. 12-200(c).

295. DoD Directive 5200.2-R. Par. 12-103.

296. E.O. 12958, § 1.3, Apr. 20, 1995.

297. *Secrecy Commission Report*, 27.

298. E.O. 12958, § 4.1(h).

299. c. 343, Title I, §102, 69 Stat. 497, Apr. 4. 1947.

300. E.O. 12333, §§ 1.3, 3.1.(1981). This superceded an earlier executive order, E.O. 12036 (Jan. 24, 1978).

301. The latest version of DCID 6/4 (formerly numbered 1/14) was issued July 2, 1998. It is reproduced at Appendix C.

302. DCID 6/4, § 1.h.

303. *Secrecy Commission Report*, 23.

304. *United States v. Sims*, 471 U.S. 159 (1985).

305. DCID 6/4, § 5.d.

306. DCID 6/4, § 6.

307. DCID 6/4, § 10.

308. DCID 6/4, § 6.c.

309. DCID 6/4, § 8.

310. The Intelligence Community, established by E.O. 12333, § 3.4 consists of 13 organizations: the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, the National Reconnaissance Office, the National Imagery and Mapping Agency, Army Intelligence, Navy Intelligence, Marine Corps Intelligence, Air Force Intelligence, the Department of State, Bureau of Intelligence and Research, the Department of Energy, the Treasury Department, Office of Intelligence Support, and the Federal Bureau of Investigation. For a more detailed description of the Intelligence Community, see the CIA Web site at *www.odci.gov/ic*.

311. DCID 6/4, Annex D, § 2.

312. Id., § 3.

313. Id., § 1.

314. Ibid.

315. CIA Regulation AR 10-16, "Appeal of Personnel Security Decisions," is not generally made available, but will be provided, if requested, to an individual appealing a security decision or their counsel.

316. AR 10-16, § e(2)(a). See Chapter 8 above.

317. E.O. 12958, § 4.1(h).

318. DoD 5200.2-R, § 1-323.

319. DoD 5200.1-R, Appendix B, "Definitions."

320. DoD 5200.2-R, § 1-323.

321. *Secrecy Commission Report*, 26.

322. DoD 5200.1-R, Appendix B, "Definitions."

323. 10 U.S.C. § 119(e), *Secrecy Commission Report,* 26.

324. *Secrecy Commission Report*, 27.

325. E.O. 12958, §§ 4.4, 5.6(c).

326. *Secrecy Commission Report,* 27; DoD 5200.2-R, § 8-101.

327. E.O. 12958, § 4.4.

328. E.O. 12958, § 4.4.

329. DoD 5200.1-R, § 1-302.

330. 10 U.S.C. § 119(e).

331. DoD 5200.1-R, § 8-103.

332. DoD 5200.1-R, § 8-103(f).

333. DoD 5200.1-R, § 8-103(e).

334. DoD 5200.1-R, § 8-108.

335. DoD 5200.2-R, Chap. 3, § 5.

336. E.O. 12968, § 2.2(b).

337. 360 U.S. 474, 508 (1959).

338. DoD 5200.2-R, § 8-200.

339. Ibid.

340. *Industrial Security Program Report.*

341. Id., pp. 8-9.

342. The background of the adoption of Executive Order 12958 is more fully discussed in Chapter 1. In summary, based on the recommendations of a Joint Security Commission for a simplified, more uniform, and more cost-effective system, Congress in 1994 amended the National Security Act of 1947 to require the President to establish procedures to govern access to classified information binding on the Executive Branch and Congress. As a result of that legislation, the President signed Executive Order 12958 on April 17, 1995, establishing a uniform system for classifying, declassifying, and safeguarding national security information.

343. Executive Order 12958, § 5.2.

344. The NISPOM has been issued as a Department of Defense Document, DoD 5220.22-M, as DoD was designated the executive agency for the program.

345. The physical safeguarding of SCI material in government is controlled by DCID 1/19, *Security Policy and Security Policy Manual for Sensitive Compartmented Information.*

346. NISPOM, Para. 1-201, 1-202.

347. Id., Para. 102-8.

348. Id., Chapter 1, Section 3.

349. Id., Para. 3-104.

350. Id., Para. 2-100.

351. Id., Para. 2-102.

352. Id., Chapter 2, Section 1.

353. Id., Chapter 2, Section 2.

354. Ibid.

355. Id., Chapter 2, Section 3.

356. Ibid.

357. Ibid.

358. Ibid.

359. Id., Para. 2-303.

360. Id., Para. 2-306.

361. Id., Para 2-311.

362. NISPOM, Chapter 5. A separate DoD regulation concerning the Information Security Program, DoD 5200.2-R, was issued in January 1997 to implement Executive Order 12958. Although binding only on the DoD, it is a model for other agency regulations. Chapter 6 of the regulation covers physical security.

363. DoD 5200.2-R, §6-304.

364. Id., §6-302.

365. NISPOM, Chap. 5, Sec. 2.

366. Id., Sec. 3.

367. DoD 5200.2-R, Appendix G.

368. NISPOM, Chapter 5, Secs. 3,8,9. DoD 5200.2-R, Appendix G gives very specific requirements for the constructions of vaults, security rooms, intrusion detection systems, and access controls, including "biometric devices", i.e., hand geometry,

retina scans, or voice recognition systems, for access to the most sensitive information.

369. NISPOM, Chapter 5, Section 4; DoD 5200.2-R, Chapter 7.

370. NISPOM, Chapter 5, Section 4; DoD 5200.2-R, Chapter 7, Section 3.

371. DoD 5200.2-R, Chapter 6, Section 5.

372. Id., Chapter 8.

373. Ibid.

374. DoD 5200.2-R, §6-309.

375. NISPOM, Chapter 11.

376. Ibid.

377. Presidential Decision Directive 63 issued May 22, 1998 is classified. A public Fact Sheet and White Paper explaining it in detail is available on the Web site of the Federation of American Scientists at *www.fas.org/irp/offdocs/.*

378. DoD 5200.2-R, §1-100.

379. DoD 5200.2-R, Appendix C, Sec. 2.

380. Id., Section 3.

381. Id., Sections 4 - 7.

382. The proliferation of protective markings for unclassified information was noted in the 1997 *Secrecy Commission Report,* 28-29.

383. P.L. 88-290, 78 Stat. 168, Mar. 26, 1964; P.L. 86-36, 73 Stat. 63, May 29, 1959, 50 U.S.C. 402, note; DoD Dir. 5210.45, May 9,1964.

384. DoD Directive 5210.48, § D.13.a.

385. DoD Directive 5210.45, § II.

386. Id., § III.

387. Ibid.

388. NSA/CSS Regulation No. 122-07, Mar. 13, 1998.

389. DoD Regulation 5210.48-R, App. B.

390. DoD Directive 5210.45 provides that a three-member board shall consider access determinations under proceedings which shall not include notice to the individual, a right to a hearing or appeal of an adverse determination. While this 1964 directive has not been withdrawn or revised, in practice it has been superceded by NSC/CSS Reg. No. 122-07 which implements Executive Order 12968.

391. NSA/CSS Reg. No. 122-07, § III, Par. 5.

392. Id., § V.

393. Id., § VI.

394. Id., § VI, Par. 17.c.

395. Id., § VI, Par. 19.

396. Id., § VI, Par. 19.

397. Id., § VI, Par. 20.

398. 50 U.S.C. § 833 (repealed, P.L. 104-201, § 1633(b)(2), 110 Stat. 2751 (1996)).

399. Atomic Energy Act of 1954, as amended, c.1073, 68 Stat. 921, 940, Aug. 30, 1954 (42 U.S.C. §§ 2011-2296).

400. Regulations of the Nuclear Regulatory Commission concerning criteria and procedures for determining eligibility for access to restricted data or national security information or on employment clearance are at 10 C.F.R. Part 10 (64 Fed. Reg. 15641, Apr. 1, 1999).

401. See Secrecy Commission Report, p. 23 (1997).

402. 42 U.S.C. § 2014(y).

403. 42 U.S.C. § 2162(d).

404. Secrecy Commission Report, p. 24.

405. Section 142(d) of the Atomic Energy Act.

406. *Secrecy Commission Report*, p. 76. Originally nuclear energy clearances were classed as "A," "B," and "C," but these designations were abandoned because it was felt that individuals might think that "B" and "C" clearances reflected on their integrity. Clearances were then designated "Q," "S" and "P," derived by reversing the first letters of the term "Personnel Security Questionnaire" (PSQ). Only the "Q" designation has survived. *A Review of the AEC Security Program, 1947-1973,* p. 90 (Div. of Security, AEC). The "L" designation derives from a "Limited" clearance that originated at the Oak Ridge facility many years ago.

407. DOE Order 472.1B, Personnel Security Activities (Mar. 24, 1997); *DOE Personnel Security Program Manual*, DOE M 472.1-1 (May 22, 1998)

408. Statistics have been provided by the DOE Office of Safeguards and Security, Office of Security Affairs. The subcategories are less than the total cases closed due to other administrative actions being taken.

409. Ibid.

410. 10 C.F.R. § 710.5.

411. 10 C.F.R. § 710.1,.2.

412. DOE Order 472.1B, Personnel Security Activities (Mar. 24, 1997); *DOE Personnel Security Program Manual,* DOE M472.1-1 (May 22, 1998).

413. 10 C.F.R. § 710.6.

414. 10 C.F.R. § 704.4(B).

415. The case of Karen Silkwood, a whistle-blower in a nuclear power plant, made into a popular movie, exemplifies this problem.

416. See Energy Reorganization Act of 1974, as amended, 42 U.S.C. § 5851.

417. DOE Implementation Guidance to 10 C.F.R. Part 10.

418. Executive Order 12968, Part 5(c) allows agency heads to provide additional review proceedings beyond those required by the order.

419. 10 C.F.R. Part 710 is being revised to conform with Executive Order 12968 and will be published in the *Federal Register* as a Notice of Proposed Rulemaking. DOE will adopt the Adjudicative Guidelines used throughout the Executive Branch which were approved by the President and issued by the Security Policy Board. They will be included in the revised regulations as Appendix B.

420. DOE Polygraph Examination Regulation, 10 C.F.R. Part 709 (64 Red. Reg. 70961-70980), Dec. 17, 1999.

421. *The Washington Post*, Page A-8, Jul. 16, 2000.

422. 10 C.F.R. § 710.8.

423. 10 C.F.R. § 710.7.

424. See endnote 20.

425. 63 Fed. Reg. 4572 (1978) (32 C.F.R. Part 147).

426. Adjudicative Guidelines issued by the Security Policy Board for government-wide application are published at 63 Fed. Reg. 4572-4580, Jan. 30, 1998 (32 C.F.R. Part 147).

427. 10 C.F.R. § 710.25(l).

428. 10 C.F.R. § 710.9.

429. 10 C.F.R. § 710.21.

430. 10 C.F.R.§ 710.5(a). Prior to the 1994 revision of the regulations, hearing officers were non-government attorneys who heard the appeals on a contract basis. This was changed as a result of a GAO report, which held that the hearing was a governmental function which should be performed by government employees. Dec. B-23756, Dec. 29, 1989.

431. 10 C.F.R. § 710.21, 710.22, 710.24.

432. 10 C.F.R. § 710.25(d). DoD hearings are conducted by the Defense Office of Hearings and Appeals (DOHA). See Chapter 6 and 7.

433. Ibid.

434. 10 C.F.R.§ 710.26(c).

435. 10 C.F.R. § 710.26(d).

436. 10 C.F.R. § 710.26(h).

437. 10 C.F R. § 710.26(l). A similar procedure is available under the rules of DOHA but, according to the Chief Judge of DOHA, has never been invoked.

438. 10 C.F.R. § 710.26(o).

439. 10 C.F.R. § 710.26(q).

440. 10 C.F.R. § 710.27(b).

441. 10 C.F.R. § 710.28(c).

442. 10 C.F.R. § 710.28(e).

443. 10 C.F.R. § 710.31.

444. DOJ Employment Security Regulations, DOJ Order 2610.2A, Par. 8 (Aug. 21, 1990).

445. 28 C.F.R. § 17.11. DOJ's regulations concerning classified national security information and access to classified information are found at 28 C.F.R. Part 17. (AG Order No 2091-17) 62 Fed. Reg. 36984, July 10, 1997. A detailed description of each official's responsibilities with respect to national security information is in DOJ's regulation concerning Security Programs and Responsibilities, DOJ Order 2600.2B, (Jul. 10, 1989).

446. 28 C.F.R. § 17.12.

447. 28 C.F.R. § 17.14.

448. 28 C.F.R. § 17.11(c).

449. 28 C.F.R. § 17.47(a).

450. 28 C.F.R. § 17.47(b).

451. 28 C.F.R. § 17.15.

452. 28 C.F.R. § 17.15.

453. 28 C.F.R. § 17.47(d).

454. 28 C.F.R. § 17.47 (e).

455. E.O. 12968, § 5.2(c).

456. 28 C.F.R. § 17.47(g).

457. 28 C.F.R. § 17.47(h),(i).

458. 28 C.F.R. 17.47. 47(f).

459. 28 C.F.R. § 17.15.

460. The Procedures may be obtained from the Chair, Department of Justice ARC, Room 1116, Main Justice Building, 950 Pennsylvania Ave. NW, Washington, DC 20530-0001.

461. Information provided during an interview with the DOJ Security and Emergency Planning Staff.

462. 28 C.F.R. § 17.41.

463. According to DOJ, although consent to disclosure of financial information is a requirement of E.O. 12968, issued in October 1995, as of May 1999 that requirement has not been implemented government-wide because the financial disclosure form had still not been finally approved and adopted.

464. 28 C.F.R. § 17.41(e).

465. DoD Directive 5220.6 (Jan. 2, 1996) refers to a memorandum of understanding between DoD and the Department of Justice and 19 other departments and agencies.

466. Information provided during an interview with the DOJ Security and Emergency Planning Staff, Jul. 29,1998.

467. Information provided by the DOJ Security and Emergency Planning Staff.

468. Information provided by the Chair, Access Review Committee.

469. Information provided during an interview with the DOJ Security and Emergency Planning Staff, Jul. 29,1998.

470. Information concerning the FBI's security program, unless otherwise referenced, was provided by a personal interview with representatives of the FBI's Office of General Counsel, Office of Public Affairs, and units dealing directly with personnel security clearance issues.

471. Information provided by the Assistant Director, OPM Investigations Service.

472. Background employment investigations of FBI Special Agents and its other employees are conducted in accordance with Part 67 of the FBI *Manual of Investigative Guidelines* (MIOG).

473. These investigations are covered by Part 259 of the MIOG.

474. Personnel and facility clearances under the Industrial Security Program are handled by the Industrial/ Facility Security Unit, Security Countermeasures Section, National security Division. FBI employee security clearances are also handled by that division.

475. See MAOP Part II, 3-1.1 and 3-1.2. The FBI, at the time of this writing, has not provided any part of its MAOP, so the description of its contents is based on information provided at a personal interview with representatives of the FBI's Office of General Counsel, Office of Public Affairs, and units dealing directly with personnel security clearance issues, as well as references to it in the FBI's *Manual of Investigative Operations and Guidance* (MIOG).

476. E.O.12968, Sec. 2.1(a)(2)(1995).

477. 32 C.F.R. § 147.10, 63 Fed. Reg. 4576 (Jan. 30, 1998).

478. MIOG Part I, Subsec. 67-7.6.

479. Id, Subsec. 67-7.8.

480. Ibid.

481. Ibid.

482. 32 C.F.R. Part 147, Attachment C to Subpart B, 63 Fed. Reg. 4578 (Jan. 30, 1998).

483. The requirement for universal polygraphing of FBI applicants was begun on May 4, 1994 according to information provided during an interview with the DOJ Office of Security and Emergency Planning. An FBI regulation, MIOG, Subsec. 76-7.9 issued earlier (1/11/85), provides that polygraphing is only to be on approval of the Assistant Director of the Inspection Division, or some other person designated by the Director, FBI, provided the exam would materially assist in the resolution of questions concerning (a) relationship or allegiance to a foreign power, (b) freedom from coercive forces, or (c) ability to abide by laws and regulations and intent to use his or her employment for FBI purposes.

484. MIOG, Subsec. 67-7.9(b)(3).

485. MIOG, Subsec. 260-2.1.

486. MIOG, Subsec. 260-1.

487. MIOG Subsec. 260-2.3.

488. MIOG Subsec. 260-2.5.

489. See Chapter 1 for a discussion of the development of the Uniform Guidelines.

490. MIOG Subsec. 260-2.1(2).

491. Information provided by a personal interview with representatives of the FBI's Office of General Counsel, Office of Public Affairs, and units dealing directly with personnel security clearance issues.

492. Ibid.

493. MIOG Subsec. 260-2.4.

494. MIOG Subsec. 260-4.

495. MIOG Subsec. 260-4.2.

496. MIOG Subsec. 260-4.

497. MIOG Subsec. 260-3.

498. MIOG Subsec. 260-3.1.

499. *Carlucci v. Doe*, 488 U.S. 93, 102 (1988).

500. *Cole v. Young,* 351 U.S. 536,542-43, (1956). (Reversing the removal of an FDA food and drug inspector who was charged with being a Communist.)

501. 5 U.S.C. § 7531. NSA, DIA and the Defense Mapping Agency were added by Memorandum of President Reagan, May 23, 1988, 53 F.R. 26023 (5 U.S.C. 7531, note).

502. *Cole v. Young,* 351 U.S. 541.

503. *Carlucci v. Doe*, 488 U.S. 104. The Supreme Court in *Cole v. Young* held that in the absence of an immediate threat of harm to the "national security," the normal dismissal procedures seem fully adequate, and the justification for summary powers disappears. 351 U.S. 546.

504. *Carlucci v. Doe*, 488 U.S. 93.

505. If an employee's clearance has been suspended, an agency may suspend the employee without pay indefinitely during the investigation of whether his clearance should be continued. *Holley v. Dept. of the Navy,* 62 M.S.P.R. 300 (MSPB 1994).

506. *Griffin v. Defense Mapping Agency*, 864 F.3d 1579, 1580 (Fed. Cir. 1989); Holley v. Dept of the Navy, supra.

507. 5 U.S.C. § 7513. *Department of the Navy v. Egan*, 484 U.S. 518 (1988).

508. 5 U.S.C. § 7532(b).

509. 5 U.S.C. § 7532(c).

510. In dictum in *Department of the Navy v. Egan,* the Court stated: "Even assuming he would be entitled to a [trial-type] hearing under § 7532, we would still consider the two procedures [comparing 5 U.S.C. § 7513] not anomalous, but merely different. 484 U.S. 533.

511. *The Federal Personnel Manual*, Chap. 732, Sec. 5-4. (*The Federal Personnel Manual* was abolished in 1993. Chapter 732 of the Code of Federal Regulations is currently under revision and is expected to contain many of the provisions that previously appeared in the FPM).

512. Ibid.

513. Ibid.

514. 5 U.S.C. § 3571.

515. 5 U.S.C. § 7312.

516. P.L. 96-456, 94 Stat. 2025, Oct. 15, 1980; 18 U.S.C. App. 3, §§ 1 - 16.

517. *United States v. Pappas,* 94 F.3d 795 (2d cir. 1996); *United States v. Wilson,* 571 F.Supp. 1422 (D.C.N.Y. 1983).

518. 18 U.S.C. App. 3, § 6(e).

519. *Security Procedures Established Pursuant to P.L. 94-456, 94 Stat. 2025 by the Chief Justice of the United States for the Protection of Classified Information.* (Hereinafter, "*Security Procedures*") (18 U.S.C. App. III, §9, note).

520. *Security Procedures*, § 2.

521. *Security Procedures*, § 4.

522. *Security Procedures*, § 5.

523. *Security Procedures*, § 6.

524. *Security Procedures*, § 9.

525. Information concerning the DOJ Court Security Section was provided during an interview with the Associate Director, Security and Emergency Planning Staff, in August 1998.

526. *Security Procedures*, § 4.

527. *Bowers v. U.S. Dept. Of Justice,* 690 F.Supp. 1483 (W.D.N.C. 1987) (inapplicable to FOIA proceeding); *United States v. Koreh,* 144 F.R.D. 218 (D.N.J. 1992)(does not apply in denaturalization proceeding).

528. 28 C.F.R. §§ 17.17, 17.46.

529. 28 C.F.R. § 17.46(c). Federal Magistrate Judges have their access eligibility determined under an agreement between DOJ and the Judicial Conference of the United States.

530. 28 C.F.R. § 17.46(d).

531. 28 C.F.R. § 17.41(a).

532. Eg., *Bowers v. U.S. Dept. of Justice, supra; United States v. Koreh, supra.*

533. Standard Form 312.

Appendix A

Sources on the Protection of National Security Information

Appendix A

Sources on the Protection of National Security Information

A. Statutes

1. National Security Act of 1947, as amended, c. 343, 61 Stat. 496, Jul. 26, 1947 (50 U.S.C. 401-432).

2. Central Intelligence Agency Act of 1949, c. 227, 63 Stat. 208 (50 U.S.C. 403a-403i) Jun. 20, 1949.

3. National Security Agency Act of 1959, 73 Stat. 63, P.L. 86-36, May 29, 1959 (50 U.S.C. 402, note).

4. Act to Permit Summary Suspension and Removal of Employees for National Security Reasons, c. 803, 64 Stat. 476, Aug. 26, 1950 (5 U.S.C. 3571,7532).

5. Internal Security Act of 1950, as amended, c. 1024, Stat. 987, Sept. 23, 1950 (50 U.S.C. 783).

6. Atomic Energy Act of 1954, as amended, c. 1073, 68 St. 919, 940-943, Aug. 30, 1954 (42 U.S.C. 2161-2166).

7. National Security Agency Act of 1959 (Personnel Security Procedures, P.L. 88-290, 78 Stat. 168-170, Mar. 26, 1964 (50 U.S.C. 831-835).

8. Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 783, Oct. 25, 1978 (50 U.S.C. 1801-1811).

9. Classified Information Procedures Act, P.L. 96-456, 94 Stat. 2025, Oct. 15, 1980 (18 U.S.C. App. 3, §§ 1 - 16).

10. Counterintelligence and Security Enhancements Act of 1994, P.L. 103-359, Title VIII, §802(a), 108 Stat. 3434, Oct. 14, 1994 (50 U.S.C. 435).

B. Executive Orders

1. E.O. 9835, Employees' Loyalty Program in the Executive Branch, Mar. 21, 1947 (12 Fed. Reg. 1935; 1947 U.S. Code Cong. Service 1997).

2. E.O. 10450, Security Requirements for Government Employment, Apr. 27, 1953. (5 U.S.C. 7311, note).

3. E.O. 10865, Safeguarding Classified Information Within Industry, Feb. 20, 1960 (50 U.S.C. 401, note).

4. E.O. 10909, amending E.O. 10865, Jan. 17, 1961 (50 U.S.C. 401, note).

5. E.O. 11905, United States Foreign Intelligence Activities, 41. Fed. Reg. 7703, Feb. 18, 1976 (superseded by E.O. 12306).

6. E.O. 11935, Citizenship Requirements for Federal Employment, Sept. 2, 1976, 5 U.S.C. 3301, note).

7. E.O.12065, Classification and Declassification of National Security Information and Material, Jun. 28, 1978, 43 Fed. Reg. 28949 (superseded by E.O. 12356).

8. E.O. 12333, United States Intelligence Activities, 46 Fed. Reg. 59941, Dec. 4, 1981 (50 U.S.C. 401, note).

9. E.O. 12356, National Security Information, Apr. 2, 1982 (50 U.S.C. 401, note) (superseded by E.O. 12958).

10. E.O. 12656, Assignment of Emergency Preparedness Responsibilities, Nov. 18, 1988, 53 F.R. 47491 (50 U.S.C. App. 2251, note).

11. E.O. 12829, National Industrial Security Program, 58 Fed. Reg. 3479, Jan. 6, 1993 (50 U.S.C. 435, note).

12. E.O. 12958, Classified National Security Information, Apr.17, 1995 (50 U.S.C. 435, note).

13. E.O. 12968, Access to Classified Information, Aug. 2, 1995 (50 U.S.C. 435, note).

C. National Security Directives

National security directives have been given different names by each administration. They were called National Security Directives (NSDs) in the Bush administration, National Security Decision Directives (NSDDs) in the Reagan administration, Presidential Directives (PDs) in the Carter administration, National Security Decision Memoranda (NSDM) in the Nixon and Ford administrations, and National Security Action Memoranda (NSAMs) in the Kennedy and Johnson administrations. They are known as President Decision Directives (PDDs) in the Clinton Administration. National Security Council Intelligence Directives (NSCIDs) are Guidance to Entire Intelligence Community.

1. PD-55, Jan. 10, 1980, Intelligence Special Access Programs: Establishment of APEX Program.

2. NSD-63, Oct. 21, 1991, Single Scope Background Investigations.

3. NSDD-19, Jan.12, 1982, Protection of Classified National Security Council and Intelligence Information.

4. NSDD-84, Mar. 11, 1983, Safeguarding National Security Information, (specified new security requirements for individuals permitted access to code word information).

5. PDD/NSC-29, Sept. 16, 1994, Security Policy Coordination - Established Security Policy Board.

6. PDD/NSC-62, May 22, 1998, Combating Terrorism.

7. PDD/NSC-63, May 22, 1998, Protecting America's Critical Infrastructures.

D. Security Policy Board Policies

1. Personnel Security Policies for Granting Access to Classified Information; Subpart A, Adjudicative Guidelines; Subpart B, Investigative Standards. 32 C.F.R. Part 147 (63 Fed. Reg. 4572, Jan. 30, 1998).

2. National Policy of Reciprocity of Facilities and Guidelines for Implementation of Reciprocity. 32 C.F.R. Part 148 (63 Fed. Reg. 4580, Jan. 30, 1998).

E. Director of Central Intelligence Directives

Directives from the Director of Central Intelligence are known as DCIDs and have government-wide application. The Director of Central Intelligence, who is the President's Chief Advisor on Intelligence, also serves in another role as the Director of the CIA.

1. DCID 1/7, Security Controls on the Dissemination of Intelligence Information, (For Official Use Only), Jun. 30, 1998.

2. DCID 1/19, Security Policy for SCI [Unclassified], Mar. 1, 1995.

3. DCID 1/20, Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information [Unclassified], Dec. 29, 1991.

4. DCID 1/21, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs) [For Official Use Only], Jul. 29, 1994.

5. DCID 3/29, Controlled Access Program Oversight Committee, Jun. 2, 1995.

6. DCID 6/2, Technical Surveillance Countermeasures [Confidential], Mar. 11, 1999

7. DCID 6/3, Protection of Sensitive Classified Information within Information Systems and Networks [Secret], Jun. 5, 1999.

8. DCID 6/3 Supplement, Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks [Secret] (Supplement to DCID 6/3), Jun. 5, 1999.

9. DCID 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI) [Unclassified] with Annexes A - F. Jul. 2, 1998.

F. Department of Defense Directives, Regulations And Manuals

1. DoD Directive 1400.5, Policy for Civilian Personnel, Mar. 21, 1983.

2. DoD Instruction 1401.1, Personnel Policy for Nonappropriated Fund Instrumentalities (NAFIS) Nov. 15, 1985.

3. DoD 1401.1-M, Personnel Policy Manual for Nonappropriated Fund Instrumentalities (NAFIS), Dec. 1998.

4. DoD Directive 5025.1, DoD Directives System, Jun. 24, 1994.

5. DoD Directive 5025.1-I, DoD Directives Systems Annual Index, Feb. 1996.

6. DoD Directive 5025.1-M, DoD Directives Systems Procedures, Aug.1994.

7. DoD Directive 5100.23, Administrative Arrangements for the National Security Agency, May 17, 1967.

8. DoD Directive 5105.42, Defense Security Service, May 13, 1999.

9. DoD Directive 5145.3, Surveillance of DoD Security Programs, Oct. 19, 1962.

10. DoD Directive 5200.1, DoD Information Security Program, Dec. 13, 1996, (delegates authority and assigns responsibilities) (32 C.F.R. Part 159).

11. DoD 5200.1-H, DoD Handbook for Writing Security Classification Guidance, Mar. 1986.

12. DoD 5200.1-I, Index of Security Classification Guides (For Official Use Only - filed in Pentagon Library Army Studies Room), Sep. 1996.

13. DoD 5200.1-M, Acquisitions Systems Protection Program, Mar. 1994.

14. DoD 5200.1-R, Information Security Program Regulation, Jan. 1997 (32 C.F.R. PART 159a).

15. DoD Directive 5200.2, Personnel Security Program, Apr. 4, 1999 (32 C.F.R. Part 156).

16. DoD Dir 5200.2-R, Personnel Security Program Regulation, Jan. 1987, as amended (32 C.F.R Part 154).

17. DoD Directive 5200.8, Security of Military Installations and Resources, Apr. 25, 1991 (assignment of authority).

18. DoD Directive 5200.8-R, Physical Security Program, May 1991.

19. DoD Directive 5200.26, Defense Investigative Program, June 12, 1979 (assignment of authority).

20. DoD Directive 5200.28, Security Requirements for Automated Information Systems, Mar. 21, 1988.

21. DoD 5200.28-M, Automated Information System Security Manual.

22. DoD Directive 5200.30, Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records, Mar. 21, 1983 (32 C.F.R Part 158).

23. DoD Directive 5200.32, Security Countermeasures (SCM) and Polygraph Education, Training and Program Support, Feb. 26, 1996 (authorizes DoDPI as the sole source of basic and advanced psycho-physiological detection of deception).

24. DoD Directive 0-5205.7, Special Access Program (SAP), Policy, Jan. 4, 1989 (for official use only - filed in Pentagon Library Army Studies Room).

25. DoD Directive 5210.2, Access to and Dissemination of Restricted Data, Jan. 12, 1978.

26. DoD Directive 5210.41, Security Policy for Protecting Nuclear Weapons, Sept. 23, 1988.

27. DoD Directive 5210.42, Nuclear Weapon Personnel Reliability Program, May 25, 1993.

28. DoD Directive 5210.45, Personnel Security in the National Security Agency, May 9, 1964.

29. DoD Directive 5210.46, DoD Building Security for the National Capital Region, Jan. 28, 1982.

30. DoD Directive 5210.48, DoD Polygraph Program, Dec. 24, 1984.

31. DoD Directive 5210.48-R, Polygraph Program Regulation, Jan. 9, 1985 (contains counterintelligence topics for polygraph).

32. DoD Directive 5210.55, DoD Presidential Support Program, Dec. 15, 1998.

33. DoD Instruction 5210.87, Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities, Nov. 30, 1998.

34. DoD Directive 5210.65, Chemical Agent Security Program, Oct. 15, 1986.

35. DoD Directive 5210.79, DoD Personnel Security Research Center (PERSEREC), Jul. 9, 1992.

36. DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Program, Feb. 2, 1992 (32 C.F.R. Part 155).

37. DoD Directive 5220.22, DoD Industrial Security Program, Dec. 8, 1980.

38. DoD Directive 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), (replaces Industrial Security Manual for Safeguarding Classified Information, 1991 ed.), Jan. 1995.

39. NISPOM Supplement (for SAP and SCI storage requirements), Feb. 1995.

40. DoD 5220.22-R, Industrial Security Regulation (establishes policies for military and civilian employees and employees of Defense contractors), Dec. 1985.

41. DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, Jun. 16, 1992.

42. DoD Directive 5230.21, Protection of Classified National Security Council and Intelligence Information, Mar. 15, 1982.

43. DoD Directive 5230.22, Control and Dissemination of Intelligence Information, Apr. 1, 1992 (for official use only - filed in Pentagon Library Army Studies Room).

44. DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, Dec. 1982.

45. 32 CFR Part 158, Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records (See DoD Dir 5200.30).

G. Other Agency Regulations and Directives

1. Air Force Instruction 31-501, Personnel Security Program Management, May 2, 1994, revised, by implementing instruction, Apr. 22, 1996.

2. Air Force Regulation 0-2, Numerical Index of Standard and Recurring Air Force Publications, Jul. 1, 1992.

3. Air Force Regulation 200-7, Sensitive Compartmented Information (SCI) Security System, Apr. 1987.

4. AFSPACECOM Regulation 200-2, The Security, Use and Dissemination of Sensitive Compartmented Information (SCI), Aug. 31, 1990.

5. Air Force Technical Application Center (AFTAC), Regulation 0-2, Numerical Index of Center Publications, Nov. 1986.

6. Army Intelligence and Security Command (INSCOM) Pamphlet 25-30, Index of Administrative Publications and Command Forms, June 25, 1991.

7. Army Regulation 380-67, Personnel Security Program, Feb. 15, 1990, amended by Ch. 3, Para. 8201.

8. Courts - Security Procedures Established Pursuant to P.L 94-456 (Classified Information Procedures Act) by the Chief Justice of the United States for the Protection of Classified Information, (18 U.S.C. App. III. § 9, note).

9. CIA Regulation AR 10-16, Appeal of Personnel Security Decisions, July 30, 1998.

10. DIA Regulation 0-2, Index of DIA Administrative Publications, Dec. 10, 1982.

11. Defense Security Service 20-1-M, Manual for Personnel Security Investigations, Jan. 1993.

12. Defense Intelligence Agency Regulation No. 22-7, Civilian Personnel Adverse Actions, Apr. 7, 1986.

13. Defense Intelligence Agency Regulation No. 22-52, Civilian Personnel, Aug. 24, 1983.

14. Defense Intelligence Agency Regulation No. 50-8, Personnel Security Program, Oct. 2, 1975.

15. Defense Security Service, DIS 31-4-R, Industrial Security Operating Regulation (ISOR), Sept. 4, 1984.

16. Department of Energy Regulation, 10 C.F.R. Part 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material, July 8, 1994.

17. Department of Energy, Nuclear Classification, and Declassification Regulation, 10 C.F.R Part 1045, 62 Fed. Reg. 68501, Dec. 31, 1997.

18. Department of Energy Polygraph Examination Regulation, 64 Fed. Reg 70961-70980, Dec. 17, 1999.

19. Department of Energy Implementation Guidance for Title 10, Code of Federal Regulations, Part 710, Subpart A.

20. DOE Order 472.1B, Personnel Security Activities, Mar. 24, 1997.

21. DOE, Personnel Security Program Manual DOE M 472.1-1, May 22, 1998.

22. Department of Justice Regulations Implementing E.O. 12958 and 12968, "Classified National Security Information and Access to Classified Information," 28 C.F.R. Part 17, §§ 17.1-17.47; 62 Fed. Reg. 36984, July 10, 1997.

23. DOJ Order 2600.2B, Security Programs and Responsibilities, July 10, 1989.

24. DOJ Order 2610.2A, Employment Security Regulations, Aug. 21, 1990.

25. Department of State Foreign Affairs Manual, 3 F.A.M. Subchap. 160, Personnel Security, May 1, 1987.

26. FBI Manual of Investigative Operations and Guidance (MIOG), Secs. 67, 259, and 260.

27. FBI Manual for Administrative Operating Procedures (MIAP).

28. Information Security Oversight Office (ISOO), Directive No. 1.

29. Navy Personnel Security Program, Security Inst. 5510.30A, Mar. 10, 1999.

30. Navy Information Security Program, SECNAV Inst. 5510.36, Mar. 17, 1999.

31. Office of Personnel Management, Personnel Security and Personnel Investigations Regulations, 5 CFR Parts 732 and 736.

32. Office of Personnel Management, Federal Personnel Manual, Personnel Suitability, Chap. 731, Personnel Security, Chap. 732, and Personnel Investigations, Chap. 736 (all now abolished).

33. USSPACECOM Regulation 200-1, The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI), Apr. 15, 1992.

34. USSAN Instruction 1-69, United States Security Authority for North Atlantic Treaty Organization Affairs, Apr. 21, 1982 (Enclosure 2 to DoD Dir 5100.55).

H. Interagency Agreements

Memorandum of Understanding between the Director, White House Military Office and the Special Assistant to the Secretary and Deputy Secretary of Defense, "White House Clearances," Jul. 30, 1980.

I. Defense Office of Hearings And Appeals Issuances

1. DOHA Additional Procedural Guidance (found as Enclosure 3 to DoD Directive 5220.6 distributed by DOHA).

2. Index to Cases Under the Industrial Personnel Security Clearance Review Program, DoD Directive 5220.6, dated Dec. 20, 1976, and prior versions, (Vol. I-V, 1963-1986).

3. Index to Cases Under the Industrial Personnel Security Clearance Review Program, DoD Directive 5220.6, dated Aug. 12, 1985 (Vol. VI- XIV, 1986-1992).

4. Index to Cases under the Industrial Personnel Security Clearance Review Program, DoD Directive 5220.6, dated Jan. 2, 1992 (Vol. XV- XX, 1992-1996).

5. Case Citator for Appeals Under the Industrial Personnel Security Clearance Review Program, DoD Directive 5220.6, dated Aug. 12, 1985 (issued June 29, 1995).

6. Review Program, DoD Directive 5220.6, dated Jan. 2, 1992 (issued Oct. 31, 1997).

7. Supplement to Index to Cases Under the Industrial Personnel Security Clearance Review Program, DoD Directive 5220.6, dated Aug. 12, 1985, (Decisions from January 1, 1989 - Dec. 30, 1994).

8. Supplement to Index to Cases Under the Industrial Personnel Security Clearance Review Program, DoD Directive 5220.6, dated Jan. 2, 1992, (Decisions from Jan. 1, 1994 – Sept. 31, 1998).

J. General Accounting Office Reports

1. Improved Executive Branch Oversight Needed for the Government's National Security Information Classification Program, LCD-78-125, dated Mar. 9, 1979.

2. Continuing Problems in DoD's Classification of National Security Information, LCD-80-16, dated Oct. 26, 1979.

3. The Central Intelligence Agency's Handling of Mandatory Review Requests Under E.O. 12065, LCD-80-51, dated Apr. 11, 1980.

4. Systematic Review for Declassification of National Security Information—Do Benefits Exceed Costs? LCD-81-3, dated Oct. 15, 1980.

5. Oversight of the Government's Security Classification Program—Some Improvements Still Needed, LCD-81-13, dated Dec. 16, 1980.

6. DoD Should Give Better Guidance and Training to Contractors Who Classify National Security Information, PLRD-81-3, dated Mar. 23, 1981.

7. Faster Processing of DoD Personal Security Clearances Could Avoid Millions in Losses, GGD-81-105, dated Sept. 15, 1981.

8. Review of Department of Defense Investigation of Leak of Classified Information to The Washington Post, GAO/GGD-83-15, dated Oct. 7, 1982.

9. Further Improvement Needed in Department of Defense Oversight of Special Access (Carve-Out) Contracts, GAO/GGD-83-43, dated Feb. 18, 1983.

10. Report Supplement to Above Report "For Official Use Only," GAO/GGD-83-43 (A), dated Feb. 18, 1983.

11. Need for Central Adjudication Facility for Security Clearances for Navy Personnel, GAO/GGD-83-66, dated May 18, 1983.

12. Effect of National Security Decision Dir-84, Safeguarding National Security Information, GAO/NSIAD-84-26, dated Oct. 18, 1983.

13. Polygraph and Prepublication Review Policies of Federal Agencies, GAO/NSIAD-84-134, dated Jun. 11, 1984.

14. Concerns Regarding the National Security Agency Secure Telephone Program, GAO/NSIAD-86-7, dated Oct. 15, 1985.

15. Department of Defense: DoD's Training Program for Polygraph Examiners, GAO/NSIAD-86-33BR, Dec. 31, 1985.

16. DoD TEMPEST Protection: Better Evaluations Needed to Determine Required Countermeasures, GAO/NSIAD-86-132, dated Jun. 27, 1986.

17. Information Security: Need for DoD Inspections of Special Access Contracts, GAO/NSIAD-86-191, dated Aug. 7, 1986.

18. Information and Personnel Security: Data on Employees Affected by Federal Security Programs, GAO/NSIAD-86-189FS, Sept. 29, 1986.

19. Information Security: Special Access Document Control at Northrop's Advanced Systems Division, GAO/NSIAD-87-79, Jun. 23, 1987.

20. Polygraph Training: DOD Program Meets Standards but Expansion Requires Better Planning, GAO/NSIAD-87-161, Sept. 18, 1987.

21. National Security: DOD Clearance Reduction and Related Issues, GAO/NSIAD-87-170BR, dated Sept. 18, 1987.

22. Information Security: Actions Taken to Improve Lockheed's Special Access Document Accountability, GAO/NSIAD-88-2BR, dated Nov. 16, 1987.

23. Information Security: Update of Data on Employees Affected by Federal Security Programs, GAO/NSIAD-89-56FS, Mar. 7, 1989.

24. Information Security: Controls over Unofficial Access to Classified Information, GAO/NSIAD-89-145, Jun. 8, 1989.

25. Due Process: Procedures for Unfavorable Suitability and Security Clearance Actions, GAO/NSIAD-90-97FS, dated Apr. 23, 1990.

26. Information Security: Disposition and Use of Classified Documents by Presidential Appointees, GAO/NSIAD-90-195, dated Sept. 28, 1990.

27. Information Security: Federal Agency Use of Nondisclosure Agreements, GAO/NSIAD-91-106FS, dated Jan. 18, 1991.

28. Defense Research: Protecting Sensitive Data and Materials at 10 Chemical and Biological Laboratories, GAO/NSIAD-91-57, dated Jul. 8, 1991.

29. Security Clearances: Due Process for Denials and Revocations by Defense, Energy, and State, GAO/NSIAD-92-99, dated May 6, 1992.

30. DoD Special Access Programs: Administrative Due Process Not Provided When Access is Denied or Revoked, GAO/NSIAD-93-162, dated May 5, 1993.

31. Administrative Due Process: Denials and Revocations of Security Clearances and Access to Special Programs, Testimony Before House Subcommittee on Civil and Constitutional Rights, Committee on Judiciary, GAO/P-NSIAD-93-14, dated May 5, 1993.

32. Background Investigations: Impediments to Consolidating Investigations and Adjudicative Functions, GAO/NSIAD-95-101, dated Mar. 24, 1995.

33. Intelligence Agencies: Selected Personnel Practices at CIA, NSA and DIA Compared with Those of Other Agencies, GAO/NSIAD 96-6, dated Mar. 11, 1996.

34. Executive Office of the President: Procedures for Acquiring Access to and Safeguarding Intelligence Information, GAO/NSIAD-98-245, dated Sept. 30, 1998.

35. DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks, GAO/NSIAD-00-12, dated Oct. 27, 1999.

K. DoD Inspector General Reports

Personnel Security in the Department of Defense: A Review of the Processes for Conducting Personnel Security Investigations and Adjudicating Security Clearances. Report No. 97-196, Jul. 25, 1997.

L. Congressional Hearings and Reports

1. Hearings on Proposed Changes to Security Clearance Programs, Mar. 9, 1989, House Committee on Post Office and Civil Service, H.R.

2. Hearings on Standards and Due Process Procedures for Granting, Denying, and Revoking Security Clearances, House Committee on Post Office and Civil Service, Subcommittee on Civil Service, House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights; Oct. 5; Nov. 2, 16, 1989; Feb. 28, Mar. 8, 1990.

3. Hearings before the House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, and House Committee on Post Office and Civil Service, Subcommittee on Civil Service Due Process in Security Clearance Determinations, May 5, 1993.

4. *United States Counterintelligence and Security Concerns--1986.* Report by the Permanent Select Committee on Intelligence, House of Representatives. H.R. Rep. 100-5, 100th Cong., 1st Sess., Feb. 4, 1987.

5. Hearings on Standards and Due Process before the Subcommittee on Legislation and National Security, House Committee on Government Operations, Mar. 18, 1992.

M. Judicial Decisions

1. Other relevant cases are collected and reported in DoD Report on Personnel Security 1993 on pp. 25-30. Older cases are collected and reported in a 1988 Due Process study by PERSEREC. (See "R, Other Sources.")

2. American Federation of Government Employees v. Schlesenger, 443 F.Supp.. 431 (D.D.C. 1978).

3. American Federation of Government Employees v. U.S. Railroad Retirement Board, 742 F.Supp. 450 (E.D. Ill 1990) (Security Questionnaire).

4. *Carlucci v. Doe,* 488 U.S. 93 (1988) (termination of employment at NSA).

5. *Cole v. Young,* 351 U.S. 536 (1956) (discharge of employee under 5 U.S.C. 7532).

6. *Department of Navy v. Egan,* 484 U.S. 518 (1988) (Executive Branch authority to grant security clearances).

7. *Dorfmont v. Brown,* 913 F.2d 1399 (9th Cir. 1990), cert. denied, 499 U.S. 905 (Appeal of DISCR Decision).

8. *Greene v. McElroy,* 360 U.S. 474 (1959) (contractor's right to a hearing).

9. *Hill v. Department of Air Force,* 844 F.2d 1407 (10th Cir. 1988), cert. denied, 488

   U.S. 825 (no right to a security clearance).

10. *Kartseva v. Dept of State,* 37 F.3d 1524 (1994, amended 1995) (Constitutional right to a hearing).

11. *National Federation of Federal Employees v. Greenberg,* 789 F. Supp. 430 (D.D.C. 1989), order vacated, 983 F. 2d 286 (D.C. Cir. 1992) (review of requirement to personal information on national agency questionnaire).

12. *Stehney v. Perry,* 101 F.3d 925 (3d Cir. 1996) (use of polygraph at NSA).

13. *United States v. Scheffer,* 523 U.S. 303 (1998) (use of polygraph in court and in connection with security clearances).

14. *Vitarelli v. Seaton,* 359 U.S. 535 (1959) (discharge of government employee under 5 U.S.C. 7532).

15. *Webster v. Doe,* 486 U.S. 592 (1988) (authority of CIA to fire; decision subject to judicial review for Constitutional claims).

N. Standard Forms

1. DIS Form 40, Alcohol and Drug Abuse Information Release and Consent to Redisclosure, May 1990.

2. Standard Form 75, Request for Preliminary Employment Data, Jan. 1989.

3. DIS Form 85, Customer Consent [to Financial Records] and Authorization for Access, Aug. 1988.

4. Standard Form 85, Questionnaire for Nonsensitive Positions, Sept. 1995.

5. Standard Form 85P, Questionnaire for Public Trust Positions, Sept. 1995.

6. Standard Form 86, Questionnaire for National Security Positions) Sept. 1995.

7. DD Form 254, Contract Security Classification Specification, Dec. 1990.

8. Standard Form 312, Classified Information Nondisclosure Agreement, Jan.1991.

9. FD Form 140, Personnel Security Questionnaire (FBI).

10. FD Form 814, Personnel Security Questionnaire for 5-Year Reinvestigations (FBI).

11. Form 444, Personal History Statement, Apr. 1988 (CIA).

12. DD Form 1847-1, Sensitive Compartmented Information Nondisclosure Agreement, Dec. 1991.

13. DoD Form 1879, Request for Personnel Security Investigation, Aug. 1999.

14. Form 4193, Sensitive Compartmented Information Nondisclosure Agreement, Aug. 24, 1983.

O. Indices of Agency Regulations

DoD Directive 5025.1-I, DOD Directives System Annual Index.

P. Books

1. *The U.S. Intelligence Community*, by Jeffrey T. Richelson, 3d Ed. (Westview Press, 1995).

2. *National Security Law*, by Stephen Dycus, Arthur L. Berney, William C. Banks, & Peter Raven-Hansen, 2d Ed. (Little Brown & Co. 1997).

Q. Law Journal Articles and Presentation Papers

1. "ABA Seminar, Security Clearance Practices, Balancing the Interests of the Government and the Individual," Sept. 18, 1990.

   a. "Administrative Due Process in the Department of the Navy Central Adjudication Facility," by Dan Jacobson. (Presentation Paper)

   b. "Applicant's Right to Backpay Resulting from Improper Loss of Security Clearance," by Dan Stormer. (Presentation Paper)

   c. "Background Investigations and Clearances in the U.S. Department of Justice," by Jerry Rubino. (Presentation Paper)

   d. "Department of Energy, Adjudication and Procedural Options for Contractor Employees," by Ernest E. Wagner. (Presentation Paper)

   e. "The DISCR Appeal Process: An Introduction and Overview," by Emilio Jaksetic, Chairman, Appeals Board. (Presentation Paper)

   f. "Mission of Defense Investigative Service," by John P. Edwards, Assistant Deputy Director of Investigations. (Presentation Paper)

   g. "Representing the Applicant at a DISCR Hearing," by William L. Bransford. (Presentation Paper)

   h. "The Role of Department Counsel in the DISCR Hearing Process," by Stuart Aly. (Presentation Paper)

   i. "The Role of the Administrative Judge in DISCR Proceedings," by Robert R. Gales, Chief Administrative Judge. (Presentation Paper)

2. "Fairness and Due Process in CIA's SCI Access Determinations," by Edmund Cohen, Deputy General Counsel, CIA, Aug. 9, 1992. (Presentation Paper)

3. "Industrial Security Clearances: Heightened Importance In A World of Corporate Acquisitions, Takeovers and Foreign Investment," by William

L. Barton & Krista L. Peterson, 18 *Public Contract Law Journal* 392, Mar. 1989.

4. "Security Clearance Determinations and Due Process," Emelio Jaksetic, 12 *George Mason L. Rev.* 171, 1990.

5. "Q Clearance: The Development of a Personnel Security Program," by Harold P. Green, *Bulletin of the Atomic Scientists*, May 1964.

6. "Oppenheimer: The Case Re-examined in the Light of Watergate," by Harold P. Green, *Bulletin of the Atomic Scientists*, Sept. 1977.

R. Other Sources

1. *A Research Survey of Privacy in the Work Place*, by David F. Linowes; University of Illinois at Urbana-Champaign, Apr. 1966.

2. *Adjudicator's Desk Top Reference* (ADR) (Security Research Center),Version 99.1, Jan. 1999. Available at *www.dss.mil/training/pub/htm.*

3. *Department of Defense Report on Personnel Security, Fiscal Year 1993*, prepared by Defense Personnel Security Research Center (PERSEREC).

4. *Due Process in Matters of Clearance Denial and Revocation: A Review of the Case Law*, by John Norton Moore, Ronald L. Plesser, & Emilio Jaksetic; Defense Personnel Security Research and Education Center (PERSEREC), Apr. 1988.

5. Due Process in Industrial Security Clearance Adjudication, A Report to the Personnel Security Committee, National Industrial Security Program by the Due Process Subcommittee, July 11, 1991.

6. Essentials of Industrial Security Management, Subcourse, DST2103, Defense Security Institute, Mar. 1987.

7. *Homosexuality and Personnel Security*, by Theodore R. Sarbin, Defense Personnel Security Research and Education Center (PERSEREC), Sept. 1991.

8. Industrial Security Letters (issued periodically by the Defense Security Service to inform users of developments in industrial security).

9. Information Security Oversight Office, General Information Pamphlet (undated).

10. Information Security Oversight Office (ISOO) Annual Report, 1989.

11. ISOO Briefing Papers on Proposed Executive Order, Classified National Security Information (Now E.O. 12958), Jan. 19, 1995.

12. Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices, Nov. 1985.

13. Matrix of Scope of Investigations, Population, and Clearance Eligibility (ENTNAC, Std NAC, NACI, SSBI, PR, Secret PR) (Printed in DoD Report of Personnel Security), 1993.

14. Memorandum on Single Scope Background Investigation (SSBI), by Nina J. Stewart, Assistant Secretary of Defense, Oct. 21, 1991.

15. National Security Strategy of the United States, White House, Aug. 1991.

16. A Review of the Atomic Energy Commission Security Program, 1947-1973, Division of Security, AEC.

17. Questions and Answers on the Defense Industrial Security Program, Defense Investigative Service, Jan. 4, 1982.

18. Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence by the Joint Security Commission, Feb. 28, 1994.

19. Report of the Commission on Protecting and Reducing Government Secrecy (Pursuant to P.L. 236, 103d Cong.), 1997.

20. Scientific Validity of Polygraph Testing, A Research Review and Evaluation, U.S. Congress, Office of Technology Assessment, Nov. 1983.

21. Security Classification of Information: Vol. 1, Introduction, History, and Adverse Impacts; Vol. 2., Principles For Classification of Information, by Arvin S. Quist, Oak Ridge K-25 Site, prepared for the Department of Energy (1989). (Vols. 3 & 4 are in preparation and will discuss Classification Management, and Control of Unclassified Information.)

22. *SSBI Source Yield: An Examination of Sources Contacted during the SSBI*, by Ralph N. Carney, Defense Personnel Security Research Center (PERSEREC), Mar. 1996.

23. Studies of the Accuracy of Security Screening Polygraph Examinations Research Division, Department of Defense Polygraph Institute (DoDPI), Mar. 24, 1989.

24. The National Industrial Security Program, A Report to the President by the Secretary of Defense, Nov. 1990.

25. To Repair or Rebuild?: Analyzing Personal Security Research Agendas. Report R-3652-USDP, Sept. 1988. Prepared for the Office of the Under Secretary of Defense for Policy by RAND, National Defense Research Institute.

S. Computer Security

1. Statutes

a. Computer Fraud and Abuse Act of 1986, 100 Stat. 1213, P.L. 99-474, Oct. 16, 1986.

b. Computer Security Act of 1987, 101 Stat. 1724, P.L. 100-235, Jan. 8, 1998.

2. Office of Management & Budget

OMB Circular, Management of Federal Information Resources, A130, Appendix III, Security of Federal AISs.

3. National Telecommunications & Information Systems Security (NTISS) Publications

a. COMPUSEC/1-87 *Security Guideline.*

b. NTISSAM *Advisory Memorandum on Office Automation.*

c. NTISSI 300 *National Policy on Control of Compromising Emanations.*

d. NTISSI 7000 *TEMPEST Countermeasures for Facilities.*

e. NTISSIC 4009 *National Information Systems Security (INFOSEC) Glossary.*

f. NACSIM 5000 *TEMPEST Fundamentals.*

g.. NACSIM 5201 *TEMPEST Guidelines for Equipment/System Design Standard.*

h. NACSIM 5203 *Guidelines for Facility Design and Red/Black Installation.*

i. NACSIM 7002 *COMSEC Guidance for ADP Systems.*

4. **National Computer Security Center (NCSC) Publications (The Rainbow Series)**

a. NCSC-WA-002-85 Personal Computer Security Considerations.

b. NCSC-TG-001 A Guide to Understanding Audit in Trusted Systems [Tan Book].

c. NCSC-TG-002 Trusted Product Evaluation- A Guide for Vendors [Bright Blue Book].

d. NCSC-TG-003 A Guide to Understanding Discretionary Access Control in Trusted Systems [Orange Book].

e. NCSC-TG-004 Glossary of Computer Security Terms [Aqua Book].

f. NCSC-TG-005 Trusted Network Interpretation [Red Book].

g. NCSC-TG-006 A Guide to Understanding Configuration Management in Trusted Systems [Orange Book].

h. NCSC-TG-007 A Guide to Understanding Design Documentation in Trusted Systems [Burgundy Book].

i. NCSC-TG-008 A Guide to Understanding Trusted Distribution in Trusted Systems [Lavender Book].

j. NCSC-TG-009 Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria [Venice Blue Book].

k. NCSC-TG-011 Trusted Network Interpretation Environments Guideline-Guidance for Applying the Trusted Network Interpretation [Red Book].

l. NCSC-TG-013 Rating Maintenance Phase Program Document [Pink Book].

m. NCSC-TG-014 Guidelines for Formal Verification Systems [Purple Book].

n. NCSC-TG-015 A Guide to Understanding Trusted Facility Management [Brown Book].

o. NCSC-TG-017 A Guide to Understanding Identification and Authentication in Trusted Systems [Lt. Blue Book].

p. NCSC-TG-018 A Guide to Understanding Object Reuse in Trusted Systems [Lt. Blue Book].

q. NCSC-TG-019 Trusted Product Evaluation Questionnaire [Blue Book].

r. NCSC-TG-020A Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System [Gray Book].

s. NCSC-TG-021 Trusted Database Management System Interpretation [Lavender Book].

t. NCSC-TG-022 A Guide to Understanding Trusted Recovery [Yellow Book].

u. NCSC-TG-025 A Guide to Understanding Data Remanence in Automated Information Systems [Green Book].

v. NCSC-TG-026 A Guide to Writing the Security Features User's Guide for Trusted Systems [Peach Book].

w. NCSC-TG-027 A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems [Turquoise Book].

x. NCSC-TG-028 Assessing Controlled Access Protection [Violet Book].

y. NCSC C-Technical Computer Viruses: Prevention, Detection, and Treatment Report 001.

z. NCSC C-Technical Integrity in Automated Information Systems (Sept. 1991) Report 79-9 i.

aa. NCSC C-Technical *The Design and Evaluation of INFOSEC Systems: The Report 32-92 Computer Security Contribution to the Composition Discussion.*

5. **Department of Defense Publications**

a. NSA/CSS Media Declassification and Destruction Manual.

b. NSA/CSS, Section 5, Degaussing Level Performance Test Procedures, Spec. LI4-4-A55.

c. Manual 130-2 Contractor Guidelines for AIS Processing of NSA SCI.

d. NSA Information Systems Security Products and Services Catalogue.

e. DoD 5200.28-M Automated Information System Security Manual.

f. DoD 5200.28 DoD Trusted Computer System Evaluation Criteria.

g. DoD 5220.22-M Supplement to National Industrial Security Program Operating Manual (NISPOM). Feb. 1995.

h. CSC-S TD-002-85 DoD Password Management Guidelines [Green Book].

i. CSC-STD-003-85 Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments [Yellow Book].

j. CSC-STD-004-85 Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements [Yellow Book].

k. CSC-STD-005-85 DoD Magnetic Remanence Security Guideline.

6. **Director of Central Intelligence Directives**

a. DCID 6/3 Protection of Sensitive Classified Information within Information Systems and Networks [Secret], Jun. 5, 1999.

b. DCID 6/3 Supplement, *Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks* [Secret] (Supplement to DCID 6/3), Jun. 5, 1999.

c. DCID 3/145 Annex B *Intelligence Community Standards for Security Labeling of Removable ADP Storage Media* [Unclassified].

7. **Directives**

National Security Decision Directive 298, National Operations Security Program, Jan. 22, 1988.

Appendix B

Personnel Security Policies for Granting Access to Classified Information, Interim Final Rule, Federal Register

APPENDIX B

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 147

RIN 0790–AG54

Personnel Security Policies for Granting Access to Classified Information

AGENCY: Department of Defense.

ACTION: Interim final rule.

SUMMARY: This rule is published to streamline security practices throughout the government, uniform adjudicative guidelines, investigative standards and guidelines for temporary access are being established. This initiative will simplify security processing and allow the deserving public to obtain a security clearance in a faster, more efficient manner.

DATES: This rule is effective March 24, 1997. Comments must be received by March 31, 1998.

ADDRESSES: Forward comments to the Security Policy Board Staff, 1215 Jefferson Davis Highway, Suite 1101, Arlington, VA 22202.

FOR FURTHER INFORMATION CONTACT: Mr. T. Thompson, 703–602–9969.

SUPPLEMENTARY INFORMATION:

Executive Order 12866, Regulatory Planning and Review

It has been determined that this interim rule (32 CFR part 147) is not a significant regulatory action. The rule does not:

(1) Have an annual effect to the economy of $100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

APPENDIX B

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive Order.

Public Law 96–354, Regulatory Flexibility Act (5 U.S.C. 601)

It has been certified that this rule is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. This part will streamline personnel security clearance procedures and make the process more efficient.

Public Law 96–511, Paperwork Reduction Act (44 U.S.C. Chapter 35)

It has been certified that this part does not impose any reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

List of Subjects in 32 CFR Part 147

Classified information, Investigations, Security measures.

Accordingly, Title 32 of the Code of Federal Regulations, Chapter I, subchapter C is amended to add part 147 to read as follows:

PART 147—ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

Subpart A—Adjudicative Guidelines

Sec.

Subpart B—Investigative Standards

Subpart C—Guidelines for Temporary Access

Authority: E.O. 12968 (60 FR 40245, 3 CFR 1995 Comp., p 391).

Subpart A—Adjudication

§ 147.1 Introduction.

The following adjudicative guidelines are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs and are to be used by government departments and agencies in all final clearance determinations.

§ 147.2 Adjudicative process.

(a) The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following actors:

(1) The nature, extent, and seriousness of the conduct;

(2) The circumstances surrounding the conduct, to include knowledgeable participation;

(3) The frequency and recency of the conduct;

(4) The individual's age and maturity at the time of the conduct;

(5) The voluntariness of participation;

(6) The presence or absence of rehabilitation and other pertinent behavioral changes;

(7) The motivation for the conduct;

(8) The potential for pressure, coercion, exploitation, or duress;

(9) The likelihood of continuation of recurrence.

(b) Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

(c) The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

(1) Guideline A: Allegiance to the United States.

(2) Guideline B: Foreign influence.

(3) Guideline C: Foreign preference.

(4) Guideline D: Sexual behavior.

(5) Guideline E: Personal conduct.

(6) Guideline F: Financial considerations.

(7) Guideline G: Alcohol consumption.

(8) Guideline H: Drug involvement.

(9) Guideline I: Emotional, mental, and personality disorders.

(10) Guideline J: Criminal conduct.

(11) Guideline K: Security violations.

(12) Guideline L: Outside activities.

(13) Guideline M: Misuse of Information Technology Systems.

(d) 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. Notwithstanding, the whole person concept, pursuit of further investigations may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

(e) 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:

(1) Voluntarily reported the information;

(2) Was truthful and complete in responding to questions;

(3) Sought assistance and followed professional guidance, where appropriate;

(4) Resolved or appears likely to favorably resolve the security concern;

(5) Has demonstrated positive changes in behavior and employment;

(6) Should have his or her access temporarily suspended pending final adjudication of the information.

(f) If after evaluating information of security concern, 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.

§ 147.3 Guideline A—Allegiance to the United States.

(a) *The concern.* An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

(2) Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(3) Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means;

(4) Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

(c) *Conditions that could mitigate security concerns include:* (1) The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(2) The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(3) Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

(4) The person has had no recent involvement or association with such activities.

§ 147.4 Guideline B—Foreign influence.

(a) *The concern.* 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 not citizens of the Untied States or 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.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

(2) Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

(3) Relatives, cohabitants, or associates who are connected with any foreign government;

(4) Failing to report, where required, associations with foreign nationals;

(5) Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

(6) Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

(7) Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

(8) A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

(c) *Conditions that could mitigate security concerns include:* (1) A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

(2) Contacts with foreign citizens are the result of official United States Government business;

(3) Contact and correspondence with foreign citizens are casual and infrequent;

(4) The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;

(5) Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

§ 147.5 Guideline C—Foreign preference.

(a) *The concern.* When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

(b) Conditions that could raise a security concern and may be disqualifying include:

(1) The exercise of dual citizenship;

(2) Possession and/or use of a foreign passport;

(3) Military service or a willingness to bear arms for a foreign country;

(4) Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

(5) Residence in a foreign country to meet citizenship requirements;

(6) Using foreign citizenship to protect financial or business interests in another country;

(7) Seeking or holding political office in the foreign country;

(8) Voting in foreign elections;

(9) Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(c) *Conditions that could mitigate security concerns include:* (1) Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(2) Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

(3) Activity is sanctioned by the United States;

(4) Individual has expressed a willingness to renounce dual citizenship.

§ 147.6 Guidance D—Sexual behavior.

(a) *The concern.* Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion.[1] Sexual orientation or

[1] The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and

preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(2) Compulsive or addictive sexual behavior when the person is unable to stop a pattern or self-destructive or high-risk behavior or that which is symptomatic of a personally disorder;

(3) Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

(4) Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

(c) *Conditions that could mitigate security concerns include:* (1) The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

(2) The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

(3) There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

(4) The behavior no longer serves as a basis for coercion, exploitation, or duress.

§ 147.7 Guideline E—Personal conduct.

(a) *The concern.* Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(1) Refusal to undergo or cooperate with required security processing, including medical and psychological testing;

(2) Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other representatives in connection with a personnel security or trustworthiness determination.

(b) *Conditions that could raise a security concern and may be disqualifying also include:* (1) Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

(2) The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(3) Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other representative in connection with a personnel security or trustworthiness determination;

(4) Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duties, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

(5) A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;

(6) Association with persons involved in criminal activity.

(c) *Conditions that could mitigate security concerns include:* (1) The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

(2) The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

(3) The individual made prompt, good faith efforts to correct the falsification before being confronted with the facts;

(4) Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

(5) The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

(6) A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

(7) Association with persons involved in criminal activities has ceased.

§ 147.8 Guideline F—Financial considerations.

(a) *The concern.* An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) A history of not meeting financial obligations;

(2) Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

(3) Inability or unwillingness to satisfy debts;

(4) Unexplained affluence;

(5) Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

(c) *Conditions that could mitigate security concerns include:* (1) The behavior was not recent;

(2) It was an isolated incident;

(3) The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downtrun, unexpected medical emergency, or a death, divorce or separation);

(4) The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

(5) The affluence resulted from a legal source;

(6) The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

§ 147.9 Guideline G—Alcohol consumption.

(a) *The concern.* Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

(2) Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

(3) Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(4) Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff

emotional, mental and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.

member of a recognized alcohol treatment program:

(5) Habitual or binge consumption of alcohol to the point of impaired judgment;

(6) Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

(c) *Conditions that could mitigate security concerns include:* (1) The alcohol related incidents do not indicate a pattern;

(2) The problem occurred a number of years ago and there is no indication of a recent problem;

(3) Positive changes in behavior supportive of sobriety;

(4) Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed impatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

§ 174.10 Guideline H—Drug involvement.

(a) *The concern.* (1) Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

(2) Drugs are defined as mood and behavior altering substances, and include:

(i) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens),

(ii) Inhalants and other similar substances.

(3) Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Any drug abuse (see above definition);

(2) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

(3) Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(4) Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(5) Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

(c) *Conditions that could mitigate security concerns include:* (1) The drug involvement was not recent;

(2) The drug involvement was an isolated or aberration event;

(3) A demonstrated intent not to abuse any drugs in the future;

(4) Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

§ 147.11 Guideline I—Emotional, mental, and personality disorders.

(a) *The concern:* Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupation functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

(2) Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

(3) A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

(4) Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

(c) *Conditions that could mitigate security concerns include:* (1) There is no indication of a current problem;

(2) Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission and has a low probability of recurrence or exacerbation;

(3) The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

§ 147.12 Guideline J—Criminal conduct.

(a) *The concern.* A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

(2) A single serious crime or multiple lesser offenses.

(c) *Conditions that could mitigate security concerns include:* (1) The criminal behavior was not recent;

(2) The crime was an isolated incident;

(3) The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

(4) The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

(5) Acquittal;

(6) There is clear evidence of successful rehabilitation.

§ 147.13 Guideline K—Security violations.

(a) *The concern.* Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

(b) *Conditions that could raise a security concern and may be disqualifying include.* (1) Unauthorized disclosure of classified information;

(2) Violations that are deliberate or multiple or due to negligence.

(c) *Conditions that could mitigate security concerns include actions that:* (1) Were inadvertent;

(2) Were isolated or infrequent;

(3) Were due to improper or inadequate training;

(4) Demonstrate a positive attitude towards the discharge of security responsibilities.

§ 147.14 Guideline L—Outside activities.

(a) *The concern.* Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's

security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

(b) *Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:* (1) A foreign country;

(2) Any foreign national;

(3) A representative of any foreign interest;

(4) Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

(c) *Conditions that could mitigate security concerns include:* (1) Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

(2) The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

§ 147.15 Guideline M—Misuse of information technology systems.

(a) *The concern.* Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Illegal or unauthorized entry into any information technology system;

(2) Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;

(3) Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

(4) Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

(c) *Conditions that could mitigate security concerns include:* (1) The misuse was not recent or significant;

(2) The conduct was unintentional or inadvertent;

(3) The introduction or removal of media was authorized;

(4) The misuse was an isolated event;

(5) The misuse was followed by a prompt, good faith effort to correct the situation.

Subpart B—Investigative Standards

§ 147.18 Introduction.

The following investigative standards are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

§ 147.19 The three standards.

There are three standards (Attachment D to this subpart part summarizes when to use each one):

(a) The investigation and reinvestigation standards for "L" access authorizations and for access to confidential and secret (including all secret-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section in 4.4 of Executive Order 12958) (60 FR 19825, 3 CFR 1995 Comp., p. 33);

(b) The investigation standard for "Q" access authorizations and for access to top secret (including top secret Special Access Programs) and Sensitive Compartmented Information;

(c) The reinvestigation standard for continued access to the levels listed in paragraph (b) of this section.

§ 147.20 Exception to periods of coverage.

Some elements of standards specify a period of coverage (e.g. seven years). Where appropriate, such coverage may be shortened to the period from the subject's eighteenth birthday to the present or to two years, whichever is longer.

§ 147.21 Expanding investigations.

Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391) and other applicable statutes and Executive Orders.

§ 147.22 Transferability.

Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements for all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

§ 147.23 Breaks in service.

If a person who requires access has been retired or separated from U.S. government employment for less than two years and is the subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391); (Attachment D to this subpart, Table 2).

§ 147.24 The national agency check.

The National Agency Check is a part of all investigations and reinvestigations. It consists of a review of:

(a) Investigative and criminal history files of the FBI, including a technical fingerprint search;

(b) OPM's Security/Suitability Investigations Index;

(c) DoD's Defense Clearance and Investigations Index;

(d) Such other national agencies (e.g., CIA, INS) as appropriate to the individual's background.

Attachment A to Subpart B—Standard A—National Agency Check With Local Agency Checks and Credit Check (NACLC)

(a) *Applicability.* Standard A applies to investigations and reinvestigations for:

(1) Access to CONFIDENTIAL and SECRET (including all SECRET-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by sect. 4.4 of Executive Order 12958) (60 FR 19825, 3 CFR 1995 Comp., p. 333);

(2) "L" access authorizations.

(b) *For Reinvestigation: When to Reinvestigate.* The reinvestigation may be initiated at any time following completion of, but not later than ten years (fifteen years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Attachment D to this subpart, Table 2, reflects the specific requirements for when to request a reinvestigation, including when there has been a break in service.)

(c) *Investigative Requirements.* Investigative requirements are as follows:

(1) *Completion of Forms:* Completion of Standard Form 86, including applicable releases and supporting documentation.

(2) *National Agency Check:* Completion of a National Agency Check.

(3) *Financial Review:* Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

(4) *Date and Place of Birth:* Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(5) *Local Agency Checks:* As a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last five years, and, if applicable, of the appropriate agency for any identified arrests.

(d) *Expanding the Investigation:* The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

Attachment B to Subpart B—Standard B—Single Scope Background Investigation (SSBI)

(a) *Applicability.* Standard B applies to initial investigations for:

(1) Access to TOP SECRET (including TOP SECRET Special Access Programs) and Sensitive Compartment Information:

(2) "Q" access authorizations.

(b) *Investigative Requirements.* Investigative requirements are as follows:

(1) *Completion of Forms:* Completion of Standard Form 86, including applicable releases and supporting documentation.

(2) *National Agency Check:* Completion of a National Agency Check.

(3) *National Agency Check for the Spouse or Cohabitant (if applicable):* Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant.

(4) *Date and Place of Birth:* Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(5) *Citizenship:* For individuals born outside the United States, verification of US citizenship directly from the appropriate registration authority; verification of US citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

(6) *Education:* Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education is a primary activity of the subject during the most recent three years.

(7) *Employment:* Verification of all employments for the past seven years: personal interviews of sources (supervisors, coworkers, or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior federal and military service, including discharge type. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

(8) *References:* Four references, of whom at least two are developed; to the extent practicable, all should have social knowledge of the subject and collectively span at least the last seven years.

(9) *Former Spouse:* An interview of any former spouse divorced within the last ten years.

(10) *Neighborhoods:* Confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

(11) *Financial Review:* Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the last seven years.

(12) *Local Agency Checks:* A check of appropriate criminal history records covering all locations where, for the last ten years, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

Note: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.

(13) *Public Records:* Verification of divorces, bankruptcies, and other court actions; whether civil or criminal, involving the subject.

(14) *Subject Interview:* A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

(15) *Polygraph (only in agencies with approved personnel security polygraph programs):* In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

(c) *Expanding the Investigation.* The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

Attachment C to Subpart B—Standard C—Single Scope Background Investigation Periodic Reinvestigation (SSBI–PR)

(a) *Applicability.* Standard C applies to reinvestigation for:

(1) *Access to TOP SECRET (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information:*

(2) "Q" access authorizations.

(b) *When to Reinvestigate.* The reinvestigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation (see Attachment D to this subpart, Table 2).

(c) *Reinvestigative Requirements.* Reinvestigative requirements are as follows:

(1) *Completion of Forms:* Completion of Standard Form 86, including applicable releases and supporting documentation.

(2) *National Agency Check:* Completion of a National Agency Check (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).

(3) *National Agency Check for the Spouse or Cohabitant (if applicable):* Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant. The National Agency Check for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.

(4) *Employment:* Verification of all employments since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employments of six months or more. For military members, all services within one branch of the armed forces will be considered as one employment, regardless of assignments.

(5) *References:* Interviews with two character references who are knowledgeable of the subject; at least one will be a developed reference. To the extent practical, both should have social knowledge of the subject and collectively span the entire period of the reinvestigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

(6) *Neighborhoods:* Interviews of two neighbors in the vicinity of the subject's most recent residence of six months or more. Confirmation of current residence regardless of length.

(7) *Financial Review:—Financial Status:* Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(ii) *Check of Treasury's Financial Data Base:* Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

(8) *Local Agency Checks:* A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (Note: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.)

(9) *Former Spouse:* An interview with any former spouse unless the divorce took place before the date of the last investigation or reinvestigation.

(10) *Public Records*: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.

(11) *Subject Interview*: A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

(d) *Expanding the Reinvestigation*: The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

Attachment D to Subpart B—Decision Tables

TABLE 1.—WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investigation required is	Using standard
Confidental Secret; "L"	None	None Out of date NACLC or SSBI.	NACLC	A
	Conf, Sec; "L"			
Top Secret, SCI; "Q"	None	None	SSBI	B
	None; Conf, Sec; "L"	Current or out of date NACLC Out of date SSBI		
	TS, SCI; "Q"		SSBI-PR	C

TABLE 2.—REINVESTIGATION REQUIREMENTS

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service of	
		0–23 months	24 month's or more
Confidential	0 to 14 years, 11 mos	None (note 1)	NACLC
	15 yrs. or more	NACLC.	
Secret; "L"	0 to 9 yrs 11 mos	None (note 1).	
	10 yrs. or more	NACLC	
Top Secret, SCI; "Q"	0 to 4 yrs. 11 mos	None (note 1)	SSBI
	5 yrs or more	SSBI-PR.	

Note: As a minimum, review an updated Standard Form 84 and applicable records. A reinvestigation (NACLC or SSBI-PR) is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968.

Subpart C—Guidelines for Temporary Access

§ 147.28 Introduction.

The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, *Access to Classified Information*, are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

§ 147.29 Temporary eligibility for access.

Based on a justified need meeting the requirements of section 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

§ 147.30 Temporary eligibility for access at the confidential and secret levels and temporary eligibility for "L" access authorization.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLC).

§ 147.31 Temporary eligibility for access at the top secret levels and temporary eligibility for "Q" access authorization: For someone who is the subject of a favorable investigation not meeting the investigative standards for access at those levels.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for a Single Scope Background Investigation (SSBI).

§ 147.32. Temporary eligibility for access at the top secret and SCI levels and temporary eligibility for "Q" access authorization: For someone who is not the subject of a current, favorable personnel or personnel-security investigation of any kind.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for

immediate submission of a request for an expedited Single Scope Background Investigation (SSBI), and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal Bureau of Investigation and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).

§ 147.33 Additional requirements by agencies.

Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968. Temporary eligibility for access is valid only at the agency granting it and at other agencies who expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968, *Access to Classified Information.*

Dated: January 22, 1998.

L.M. Bynum,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 98–1955 Filed 1–29–98; 8:45 am]

BILLING CODE 5000–04–M

Appendix C

Director of Central Intelligence Directive 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)

UNCLASSIFIED

Director of Central Intelligence Directive

Type: 6 Number: 4

Subject: PERSONNEL SECURITY STANDARDS

Category: 6 - Security

Effective Date: 07/02/98

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/4[1]

PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI)

This directive supersedes Director of Central Intelligence Directive 1/14, as amended 12 August 1994.

A complete copy of DCID 6/4 now consists of the basic DCID and Annexes A through E, as follows:

- Annex A - Investigative Standards for Background Investigations for Access to Classified Information.
- Annex B - Quality Control Guidelines for the Single Scope Background Investigation.
- Annex C - Adjudication Guidelines for Determining Eligibility for Access to Classified Information.
- Annex D - Appeals Procedures: Denial or Revocation of Access.
- Annex E - Standards for SCI Security Awareness Programs in the US Intelligence Community.
- Annex F - Reciprocity of SCI Eligibility Determinations (Annex F was created subsequent to the creation of the DCID. The DCI approved Annex F on 13 Oct 99.)

[1] DCID 1/14 was renumbered 6/4 by the Director of Central Intelligence (DCI) and the Deputy Director of Central Intelligence for Community Management on 13 Oct 99, to more closely align the DCID with the new category structure as defined in DCID 1/1. This action was accomplished in conjunction with the DCI approving the newly created Annex F, "Reciprocity of SCI Eligibility Determinations".

The President approved the Adjudicative Guidelines, Temporary Eligibility Standards and Investigative Standards required by Executive Order 12968 on March 24, 1997. This revised DCID incorporates the President's policy documents verbatim, at Annexes A and C, to promote the use of these common and consistent standards for government-wide security background investigations. These two annexes should be read in the context of the Director of Central Intelligence (DCI) special authorities governing access eligibility to SCI, although the actual wording addresses a broader application to clearance actions.

The DCI exercises authority derived from statute and executive order over access eligibility to SCI and delegates this authority to Determination Authorities through Senior Officials of the Intelligence Community. (See Definitions.) Nothing in this directive or its annexes shall be deemed to preclude the DCI or the DDCI under the authority of the National Security Act of 1947, as amended, from taking any actions regarding an individual's SCI access.

Pursuant to the provisions of the National Security Act of 1947, as amended, and Executive Orders 12333 and 12968, the following personnel security guidelines, procedures, standards, and continuing security programs are hereby established for all US Government civilian and military personnel, consultants, contractors, employees of contractors, and other individuals who require access to SCI. Individual departments and agencies may establish such additional security steps as may be deemed necessary and appropriate to resolve issues and/or address employment standards unique to them to ensure that effective security is maintained.

1. Definitions.

a. Cohabitant--A person living in a spouse-like relationship with the individual requiring SCI information.

b. Compelling Need--A signed determination by a Senior Official of the Intelligence Community (SOIC) or his/her designee that the services of an individual are deemed essential to operation or mission accomplishment.

c. Risk Assessment--A written evaluation supporting the adjudicative process, especially when a significant exception to a Personnel Security Standard is being considered. This assessment should consist of an evaluation from security, counterintelligence, and other technical or management experts as appropriate, and should contrast the compelling national security benefit of an individual accessed to SCI with the risk.

d. Determination Authority--A designee of a SOIC with responsibility for decisions rendered with respect to SCI access eligibility or ineligibility.

e. Immediate Family--The spouse, parents, siblings, children, and cohabitant of the individual requiring SCI access.

f. Intelligence Community--Those US Government organizations and activities identified in the National Security Act of 1947, as amended, 50 USC 401a(4), EO 12333, or successor orders, as making up such a Community.

g. Senior Officials of the Intelligence Community (SOICs)--The heads of organizations or activities within the Intelligence Community, as defined by the National Security Act of 1947, as amended, 50 USC 401a(4), and EO 12333.

h. Sensitive Compartmented Information--Classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems, established by the DCI.

2. Purpose.

The purpose of this directive is to enhance the security protection of SCI through the application of personnel security standards, procedures, and continuing security programs.

3. Applicability.

The provisions of this directive will apply to all persons (other than elected officials of the US Government, to include elected State Governors as may be required on an individual basis, Federal judges, and those individuals for whom the DCI makes a specific exception) without regard to a civilian or military status, form of employment, official rank or position, or length of service. This directive does not apply to situations involving the duly authorized disclosure of SCI to representatives of foreign governments and international organizations.

4. General.

a. The granting of access to SCI will be controlled under the strictest application of the "need-to-know" principle and in accordance with the personnel security standards and procedures set forth in this directive.

b. In accordance with DCID 1/19, "Security Policy for Sensitive Compartmented Information," and its supplement, "DCID 1/19 Security Policy Manual," those approved for access to SCI are required to sign a DCI-authorized nondisclosure agreement that includes a provision for prepublication review as a condition of access to SCI.

5. Personnel Security Standards.

Criteria for security approval of an individual on a need-to-know basis for access to SCI are as follows:

a. The individual requiring access to SCI must be a US citizen.

b. The individual's immediate family must also be US citizens.

c. Members of the individual's immediate family and any other persons to whom he or she is bound by affection or obligation should neither be subject to physical, mental, or other forms of duress by a foreign power or by persons who may be or have been engaged in criminal activity, nor advocate the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

d. The individual must be stable; trustworthy; reliable; of excellent character, judgment, and discretion; and of unquestioned loyalty to the United States.

6. Exceptions to Personnel Security Standards.

Any exception to the Personnel Security Standards will be a common sense determination based on the fact that the available information supports a finding that the specific risk to national security is manageable in the specific case for which the exception is granted. The organization determining that an exception is warranted will document their finding in the individual's security record. As appropriate, a risk assessment, normally directed by the Determination Authority, may be required to aid in the determination of the appropriateness of granting an exception to one of the Personnel Security Standards. If accomplished, this assessment should become a part of the individual's security record.

a. The DCI is the exclusive authority for granting an exception to the requirement that the Subject be a US citizen.

b. The affected SOIC or specified designee may grant exception to the standard requiring US citizenship for the family members of an individual proposed for SCI access, as well as the standard requiring individuals to which Subject is bound by affection or obligation be free of any form of duress.

c. Exceptions to the US citizenship requirement for individuals to be accessed to SCI and their immediate family members shall require certification of a compelling need. This exception should be based upon a specific national security requirement and a certification of compelling need.

7. Investigative Requirements and Standards.

a. The investigation conducted on an individual under consideration for access to SCI will conform to the requirements of a Single Scope Background Investigation (SSBI) as defined in Annex A, "Investigative Standards for Background Investigations for Access to Classified Information." Quality Control procedures relevant to investigations are defined in Annex B, "Quality Control Guidelines for the Single Scope Background Investigation."

b. When conditions indicate, investigation of immediate family members will be conducted to the extent necessary to permit a determination by the adjudicating agency that the provisions of paragraph 5 of this directive are met.

c. Where a previous investigation has been conducted within the past five years that meets the standards of Annex A, it will serve as a basis for granting access approval except where there is substantial information indicating that the employee may not satisfy the adjudicative guidelines in Annex C. If a previous investigation does not meet the Annex A standards, if it is more than five years old, or if there is a break in SCI access of two years or more, a current investigation will be required but may be limited to that necessary to bring the individual's file up-to-date in accordance with the investigative requirements set forth in Annex A of this directive, paragraphs 6 and 10. The up-dating process may be limited to review of applicable records, starting with an updated SF-86, and involve reinvestigation only when it appears the person may no longer satisfy standards for access under this directive. Should new information be developed during the current investigation that bears unfavorably on the individual's activities covered by the previous investigation, the current inquiries will be expanded as necessary to develop full details of this information.

d. Programs will be instituted requiring the periodic reinvestigation (PR) of personnel provided access to SCI. These SSBI-PRs will be conducted in accordance with the procedures and scope contained in the section of Annex A defining the SSBI-PR. The SSBI-PR may be expanded as necessary to resolve outstanding issues.

e. Notwithstanding the status of an individual's background investigation, departments and agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary by the department or agency head to be in the national security interest of the United States. Where they exist, such polygraph programs shall be characterized by unified training and certification as well as by coordination of scope, applicability and fairness issues to promote consistency, reciprocity and due process.

f. In those cases in which the individual has lived outside of the United States for a substantial period, a thorough

assessment of the adequacy of the investigation in terms of fulfillment of the investigative requirements and judicious review of the information therein must be made before an exception is considered.

8. Temporary Eligibility for Access to SCI.

a. In exceptional cases, including national emergency situations and hostilities involving US personnel, the SOIC or his designee may determine that it is necessary or advisable in the national interest to authorize temporary access to SCI before completion of the SSBI. In this situation, the procedures contained in the Annex A section entitled "Investigative Standards for Temporary Eligibility for Access" will be complied with before temporary access is permitted. A personal interview of the individual by trained security, investigative, or counterintelligence personnel will be conducted wherever possible and practicable.

b. The SSBI and final evaluation will be completed at the earliest practicable moment unless an exception is granted by the DCI. Temporary eligibility for access is valid only at the agency granting it and other agencies which expressly agree to accept it and acknowledge understanding of its investigative basis. Therefore, certification to other organizations of individuals authorized temporary access will include explicit notification of the fact.

c. Temporary eligibility for access may be granted only to SCI necessary for the individual to perform authorized functions. Therefore, indoctrination briefings will be modified to the basic information necessary to ensure protection of the SCI to which the individual will be exposed, and appropriate nondisclosure agreements signed.

9. Reporting Requirements.

Individuals who hold SCI access have special responsibilities and obligations to report to their cognizant security officer, in writing and when feasible in advance, activities, conduct or employment that could conflict with their ability to protect classified information from unauthorized disclosure or counterintelligence threats. A more detailed explanation and a listing of an individual's responsibilities and reporting requirements are contained in Annex E. In addition, initial and updated security documents (e.g. Statement of Personal History, Questionnaire for National Security Positions, Security Clearance Application) and security records shall include details of such employment, activities, associations and/or conduct to facilitate appropriate investigation and evaluation to determine whether the circumstances create an unacceptable risk to the security of SCI or of unauthorized disclosure. Annex C, Guideline L, "Outside Activities," summarizes the concern.

10. Determinations of Access Eligibility.

The evaluation of the information developed by investigation of an individual's loyalty and suitability will be accomplished by trained professional adjudicators under the cognizance of the SOIC concerned. When all other information developed on an individual is favorable, a minor investigative requirement that has not been met should not preclude a favorable access determination by an authorized adjudicative authority. In all evaluations, the protection of the national security is paramount. Any doubt concerning personnel having access to SCI should be resolved in favor of the national security, and the access should be denied or revoked. The ultimate determination of whether the granting of access is clearly consistent with the interest of national security will be an overall common sense determination based on all available information. The adjudicative guidelines for determining eligibility for access to SCI are contained in Annex C.

11. Appeals Procedures.

Annex D prescribes common appeals procedures to be followed when an individual's SCI access has been denied or revoked.

12. Continuing Security Programs.

a. To facilitate attainment of appropriate standards of personnel security and to augment both the access approval criteria and the investigative requirements established by this directive, member departments and agencies shall institute continuing security programs based on risk management principles for all individuals having access to SCI. In addition to security indoctrinations (see Annex E, "Standards for SCI Security Awareness Programs in the US Intelligence Community"), these programs will be tailored to create mutually supporting procedures to identify and resolve issues which bring into question an individual's loyalty and integrity or suggest the possibility of his or her being subject to undue influence or duress through foreign relationships or exploitable personal conduct. These programs should include the capacity for member departments and agencies to monitor the individual's performance in a tailored program against the eligibility criteria and adjudicative standards when unresolved concerns are present. When an individual is assigned to perform sensitive work requiring access to SCI, the SOIC for the department, agency, or government program to which the individual is assigned will assume security supervision of that individual throughout the period of his or her assignment.

b. The continuing security programs will include the following:

(1) Individuals are required to inform the department or agency that grants their SCI access about any personal problem or situation that may have a possible bearing on their eligibility for continued access to SCI and to seek appropriate guidance and assistance. Security guidance should be provided by an official who understands both the eligibility issues involved, and the unique sensitivities of the specific SCI program being supported. As appropriate, tailored monitoring programs should be established to ensure that individuals actively resolve problems which have led to concern about their continued eligibility for access. An individual participating in a monitoring program with a particular department or agency does not meet the criteria for automatic reciprocal acceptance of SCI eligibility as established by Executive Order 12968. In these situations, each organization should make their own determination of eligibility.

(2) SCI security education programs of the member departments and agencies will be established and maintained pursuant to the requirements of Annex E of this directive.

(3) Security awareness programs for supervisory personnel will be established and maintained to ensure that supervisory personnel recognize and discharge their special responsibility to safeguard SCI, including the need to assess continued eligibility for SCI access. These programs will provide practical guidance on indicators that may signal matters of security concern. Specific instructions concerning reporting procedures will be disseminated to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the individual concerned to neutralize his or her vulnerability.

(4) Security review programs will ensure that appropriate security authorities always receive and exchange, in a timely manner, all information, including lead information, bearing on the security posture of persons having access to SCI. Personal history information will be kept current. Security and related files will be kept under continuing review.

(5) Where permitted by agency policy, security review programs may include the use of polygraph examinations conducted by a qualified polygraph examiner.

c. Whenever adverse or derogatory information is discovered or inconsistencies arise that could impact on an individual's security status, appropriate investigation will be conducted on a timely basis. The investigation will be of sufficient scope necessary to resolve the specific adverse or derogatory information or inconsistency in question so that a determination can be made as to whether the individual's continued utilization in activities requiring SCI is clearly consistent with the interest of national security.

13. Implementation.

Existing directives, regulations, agreements, and other guidance governing access to SCI as defined herein will be revised accordingly.

/S/
Director of Central Intelligence

2 July 1998
Date

ANNEX A[2]

Investigative Standards for Background Investigations for Access to Classified Information

1. Introduction.

The following investigative standards are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs), and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

2. The Three Standards.

There are three standards (Table 1 in the Appendix summarizes when to use each one):

a. The investigation and reinvestigation standards for "L" access authorizations and for access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by sect. 4.4 of Executive Order 12958);

b. The investigation standard for "Q" access authorizations and for access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

c. The reinvestigation standard for continued access to the levels listed in para. 2(b).

3. Exception to Periods of Coverage.

Some elements of standards specify a period of coverage (e.g., seven years). Where appropriate, such coverage may be shortened to the period from the Subject's eighteenth birthday to the present or to two years, whichever is longer.

---

[2] The content of this Annex is taken verbatim from the Presidentially approved Investigative Standards and Temporary Eligibility Standards and should be read in the context of access eligibility to SCI, although the actual wording addresses a broader application to clearance actions.

4. Expanding Investigations.

Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and Executive Orders.

5. Transferability.

Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements of all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

6. Breaks in Service.

If a person who requires access has been retired or separated from US Government employment for less than two years and is the Subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968 (see Table 2).

7. The National Agency Check.

The National Agency Check is part of all investigations and reinvestigations. It consists of a review of:

a. Investigative and criminal history files of the FBI, including a technical fingerprint search;

b. OPM's Security/Suitability Investigations Index;

c. DoD's Defense Clearance and Investigations Index; and

d. Such other national agencies (e.g., CIA, INS) as appropriate to the individual's background.

STANDARD A
National Agency Check with Local Agency Checks and Credit Check (NACLC)

8. Applicability.

Standard A applies to investigations and reinvestigations for:

a. Access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by sect. 4.4 of Executive Order 12958), and

b. "L" access authorizations.

9. For Reinvestigations: When to Reinvestigate.

The reinvestigation may be initiated at any time following completion of, but not later than ten years (fifteen years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation, including when there has been a break in service.)

10. Investigative Requirements.

Investigative requirements are as follows:

a. Completion of forms: completion of Standard Form 86, including applicable releases and supporting documentation.

b. National Agency Check: completion of a National Agency Check.

c. Financial Review: verification of the Subject's financial status, including credit bureau checks covering all locations where the Subject has resided, been employed, or attended school for six months or more for the past seven years.

d. Date and Place of Birth: corroboration of date and place of birth through a check of appropriate documentation, if *not* completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

e. Local Agency Checks: as a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the Subject has lived, worked, and/or attended school within the last five years, and if applicable, of the appropriate agency for any identified arrests.

11. Expanding the Investigation.

The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

STANDARD B
Single Scope Background Investigation (SSBI)

12. Applicability.

Standard B applies to initial investigations for:

a. Access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

b. "Q" access authorizations.

13. Investigative Requirements.

Investigative requirements are as follows:

a. Completion of Forms: completion of Standard Form 86, including applicable releases and supporting documentation.

b. National Agency Check: completion of a National Agency Check.

c. National Agency Check for the Spouse or Cohabitant (if applicable): completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant.

d. Date and Place of Birth: corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

e. Citizenship: for individuals born outside the United States, verification of US citizenship directly from the appropriate registration authority; verification of US citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

f. Education: corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education is a primary activity of the Subject during the most recent three years.

g. Employment: verification of all employments for the past seven years; personal interviews of sources (supervisors, coworkers, or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior federal and military service, including discharge type. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

h. References: four references, of whom at least two are developed; to the extent practicable, all should have social knowledge of the Subject and collectively span at least the last seven years.

i. Former Spouse: an interview of any former spouse divorced within the last ten years.

j. Neighborhoods: confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

k. Financial Review: verification of the Subject's financial status, including credit bureau checks covering all locations where Subject has resided, been employed, and/or attended school for six months or more for the last seven years.

l. Local Agency Checks: a check of appropriate criminal history records covering all locations where, for the last ten years, the Subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (NOTE: If no residence, employment or education exceeds six months, local agency checks should be performed as deemed appropriate.)

m. Public Records: verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the Subject.

n. Subject Interview: a Subject Interview, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional Subject Interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

o. Polygraph (only agencies with approved personnel security polygraph programs): in departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

14. Expanding the Investigation.

The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professional, and law enforcement professionals may be conducted.

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

15. Applicability.

Standard C applies to reinvestigations for:

a. Access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

b. "Q" access authorizations.

16. When to Reinvestigate.

The reinvestigation may be initiated at any time following completion of, but not later than five years from date of, the previous investigation (see Table 2).

17. Reinvestigative Requirements.

Reinvestigative requirements are as follows:

a. Completion of Forms: completion of Standard Form 86, including applicable releases and supporting documentation.

b. National Agency Check: completion of a National Agency Check (fingerprint cards are required *only* if there has not been a previous valid technical check of the FBI).

c. National Agency Check for the Spouse or Cohabitant (if applicable): completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant. The National Agency Check for the spouse or cohabitant is *not* required if already completed in conjunction with a previous investigation or reinvestigation.

d. Employment: verification of all employments since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employments of six months or more. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

e. References: interviews with two character references who are knowledgeable of the Subject; at least one will be a developed reference. To the extent practical, both should have social knowledge of the Subject and collectively span the entire period of the investigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

f. Neighborhoods: interviews of two neighbors in the vicinity of the Subject's most recent residence of six months or more. Confirmation of current residence regardless of length.

g. Financial Review:

(1) Financial Status: verification of the Subject's financial status, including credit bureau checks covering all locations where Subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(2) Check of Treasury's Financial Database: Agencies

may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated databases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

h. Local Agency Checks: a check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the Subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (NOTE: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.)

i. Former Spouse: an interview with any former spouse unless the divorce took place before the date of the last investigation or reinvestigation.

j. Public Records: verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the Subject since the date of the last investigation.

k. Subject Interviews: a Subject Interview, conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional Subject Interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

18. Expanding the Reinvestigation.

The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

DCID 6/4

Appendix

Decision Tables

TABLE 1: WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investigation required is	Using standard
CONFIDENTIAL SECRET; "L"	none	none	NACLC	A
	CONF, SEC; "L"	out of date NACLC or SSBI		
TOP SECRET, QSI; "Q"	none	none	SSBI	B
	none; CONF, SEC; "L"	current or out of date NACLC		
	TS, SCI; "Q"	out of date SSBI	SSBI-PR	C

TABLE 2: REINVESTIGATION REQUIREMENTS

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service of ____	
		0-23 months	24 months or more
CONFIDENTIAL	0 to 14 yrs. 11 mos.	none (NOTE 1)	NACLC
	15 yrs. Or more	NACLC	
SECRET; "L"	0 to 9 yrs. 11 mos.	none (NOTE 1)	
	10 yrs. Or more	NACLC	
TOP SECRET, SCI; "Q"	0 to 4 yrs. 11 mos.	none (NOTE 1)	SSBI
	5 yrs. Or more	SSBI-PR	

NOTE 1: As a minimum, review an updated Std. Fm. 86 and applicable records. A reinvestigation (NACLC or SSBI-PR) is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968.

DCID 6/4

Investigative Standards for Temporary Eligibility for Access

1. Introduction.

The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, "Access to Classified Information", are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

2. Temporary Eligibility for Access.

Based on a justified need meeting the requirements of section 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

3. Temporary Eligibility for Access at the CONFIDENTIAL and SECRET Levels and Temporary Eligibility for "L" Access Authorization.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLC).

4. Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization: For Someone who is the Subject of a Favorable Investigation not Meeting the Investigative Standards for Access at those Levels.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for a Single Scope Background Investigation (SSBI).

5. Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization: For Someone who is not the Subject of a current, favorable personnel or Personnel Security Investigation of any kind.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited SSBI, and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal Bureau of Investigation and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).

6. Additional Requirements by Agencies.

Temporary eligibility for access must satisfy these minimum investigations standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968. Temporary eligibility for access is valid only at the agency granting it and at other agencies who expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968, "Access to Classified Information."

ANNEX B

Quality Control Guidelines for the Single Scope Background Investigation

1. Guidelines.

In accordance with the requirements of DCID 6/4 , this document sets out guidelines to maintain quality standards for the Single Scope Background Investigation (SSBI). These guidelines assume the adjudicator's perspective because the adjudicator is the ultimate customer for the SSBI. The guidelines are divided into:

- Definition of Quality
- Conduct of the Interview
- Collection Requirements (Coverage)
- Quality Control Activities.

SOICs will ensure that investigative personnel employed by or assigned or detailed to their agencies/departments receive adequate initial and ongoing training in investigation and interrogation techniques, as well as familiarization with counterintelligence issues that may arise during investigation. Training should also incorporate findings of contemporary research in personnel security and medical disciplines and, in addition, evolving legal issues that may impact investigation collection requirements. As much as possible, training should be conducted as a joint effort with other investigative entities supporting the Intelligence Community, to facilitate information sharing and to enhance reciprocity.

2. Definition of Quality.

A quality investigation is a thorough and comprehensive collection of favorable and unfavorable information from a variety of sources, past and present, that may include employment(s), reference(s), neighborhood(s), credit, police, and the Subject.

The determination of eligibility for access to sensitive compartmented information is a discretionary determination using the whole person concept that such access is clearly in the interests of the national security. Accordingly, the investigation will be comprehensive and in such detail so as to affirmatively address unquestioned loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and

willingness and ability to abide by regulations governing the use, handling and protection of sensitive compartmented information.

3. Conduct of the Interview

The quality of the investigation depends on the investigator's ability to elicit information from a source knowledgeable about the Subject. This is basic to the conduct of any interview. The investigator should plan and execute each interview so as to obtain the maximum amount of information from a source. Available sources should be selected from each area of coverage to ensure that pertinent information about the Subject's entire background is developed.

The investigator should conduct the interview in person and find a suitable location that protects privacy. Telephonic interviews are strongly discouraged; however, occasionally exigent circumstances may dictate that the interviews be conducted by telephone. If a telephonic interview is necessary, the report should always state why the interview was not conducted in person.

The investigator should initially advise the source of the reason/purpose for the investigation and should attempt to establish a degree of confidence in the source(s) that will promote a high level of rapport and cooperation.

The investigator should also advise the source about the Privacy Act of 1974, before completing the interview, since the source needs to understand that the Subject of the investigation has the right to review information provided by a source and has the right to know a source's identity, unless the source requests confidentiality.

4. Collection Requirement (Coverage)

a. For all Sources.

Investigators should establish the duration and nature of association between the source and the Subject to assess the source's extent of knowledge. The investigator should always secure the source's full name and any other appropriate identifying data, particularly in the case of a source with a common name. All derogatory or noteworthy information concerning the Subject of the investigation that is provided by a source should be fully explored in the interview, including elicitation of the names of any corroborating sources or record information that will substantiate any derogatory testimony provided by the source. For all sources, the report should indicate what issue areas were covered and whether the information provided was favorable or unfavorable.

b. For References and Neighbors.

Depending on the source's degree of association, investigators should ask each reference or neighbor relevant information regarding the Subject's:

(1) Family, citizenship, education, employment, residence history, and military service.

(2) Reputation, character, honesty, trustworthiness, integrity, discretion, reliability, and temperament.

(3) Financial stability, organizational affiliations, and whether there is a history of mental, emotional, or physical health problems.

(4) Whether the Subject exhibits a pattern of excessive use of alcohol or has ever used illegal drugs or abused prescription drugs.

(5) Activities which indicate a lack of discretion or demonstrate poor judgment, a character flaw, or a personality disorder.

(6) Participation in criminal activity or an altercation with law enforcement agencies.

(7) Travels abroad for business or pleasure and degree of contact with foreign nationals.

(8) Unquestioned loyalty to the United States.

If a Subject has had access to classified information and a source is in a position to know, the investigator should ask whether the Subject properly handles classified information or has ever had a security violation. Finally, the investigator should ask if the source can recommend the Subject for a position of trust and responsibility with the US Government or, in the case of a contractor, can the Subject be trusted with classified information. The investigator should conclude the interview by asking the source to provide names of additional references.

c. Follow-up Questions.

If a source provides noteworthy or derogatory information to questions in any of the above areas of consideration, the investigator should ask follow-up questions as necessary to elicit all available information. The investigator should report as fully as possible:

(1) The nature, extent, and seriousness of the conduct.

(2) The motivation for and the circumstances surrounding the conduct.

(3) The frequency and recency of the conduct.

(4) The Subject's age and maturity at the time of the conduct.

(5) Whether the conduct was voluntary or whether there was pressure, coercion, or exploitation leading to the conduct.

(6) Whether the Subject has been rehabilitated or has exhibited other pertinent behavioral changes since the conduct.

If the Subject has ended the questionable conduct, the investigator should attempt to determine the motivation for positive change. The investigator should also attempt to establish whether there may be personal animosity or bias towards the Subject on the part of the source(s). The investigator should supply any available documentary evidence relating to the conduct in addition to the report of the source.

d. For Employment References.

The investigator should identify and interview the best source(s) available. These employment references should include, but are not limited to, the Subject's immediate supervisor, coworker(s), and other persons with frequent professional contact. Where appropriate, the investigator should pursue the same line of inquiry as with references and neighbors. In particular, the investigator should inquire regarding:

(1) Whether the Subject is willing to abide by company policies and regulations.

(2) Whether the Subject appropriately safeguards the employer's proprietary/sensitive information.

(3) Whether the Subject is financially stable.

(4) Whether the Subject has a history of substance abuse, to include alcohol, and/or prescription drugs.

(5) Whether the Subject has been involved in any criminal activity.

(6) Whether the Subject is reliable and eligible for re-hire.

The investigator should obtain any available documentary evidence to support the report of the source(s).

e. For Subject Interviews.

The Subject is the best source of information about himself/herself. Hence, the investigator should explore with the Subject the same line of inquiry she/he pursues with a reference, neighborhood, and employment source(s). The investigator should obtain the Subject's version of the details surrounding all issues arising either in the course of the interview or in other parts of the investigation that have been completed by the time of the Subject Interview and report them completely. The investigator should inquire regarding:

(1) What happened and why.

(2) Where, when, how, and how often it happened.

(3) Who else was involved.

(4) Was the conduct voluntary.

Of particular value to the adjudicator is evidence that the Subject is being contradictory or dissembling. If the Subject claims to have ended the conduct, the investigator should attempt to determine the motivation for positive change. The investigator should report only the facts.

5. Quality Control Activities.

Quality control activities are designed to ensure that a high quality investigation and report have been provided. The following management tools can be used by investigative agencies to ensure quality investigations, and other techniques may be appropriate:

a. Case Review.

Case review consists of a supervisory review of the investigative requirements and the investigation to ensure that all coverage has been met using the best available sources. Depending on the agency, the investigative review may be conducted by the investigator's supervisor or by a quality assurance or assessment team.

b. Ride-Along Program.

In ride-along programs, supervisors and/or senior agents accompany the investigator, observing the investigator's performance, focusing on whether the investigator:

(1) Uses proper/acceptable investigative techniques.

(2) Explores all relevant issues.

(3) Possesses a demeanor that reflects positively on the investigative agency.

c. Source Recontact.

The supervisory element may select from a sample of an investigator's cases and contact some or all of the sources. The source is queried regarding the investigator's professionalism, line of questioning, adherence to established policies and procedures, and thoroughness. Both written and telephonic re-contact are acceptable.

These recommended monitoring activities ensure adequate training of investigators, acceptable supervisory oversight, and proper professionalism while conducting the investigation. They also ensure that the standards of investigative coverage are satisfactorily met.

DCID 6/4

ANNEX C[1]

Adjudicative Guidelines for Determining Eligibility for Access to Classified Information

1. Introduction.

The following adjudicative guidelines are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs) and are to be used by government departments and agencies in all final clearance determinations.

2. The Adjudicative Process.

a. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1) The nature, extent, and seriousness of the conduct;

(2) The circumstances surrounding the conduct, to include knowledgeable participation;

(3) The frequency and recency of the conduct;

(4) The individual's age and maturity at the time of the conduct;

(5) The voluntariness of participation;

(6) The presence or absence of rehabilitation and other pertinent behavioral changes;

(7) The motivation for the conduct;

[1] The content of this Annex is taken verbatim from the Presidentially approved Adjudicative Guidelines and should be read in the context of access eligibility to SCI, although the actual wording addresses a broader application to clearance actions.

(8) The potential for pressure, coercion, exploitation, or duress; and

(9) The likelihood of continuation or recurrence.

b. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

c. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

(1) GUIDELINE A: Allegiance to the United States;

(2) GUIDELINE B: Foreign influence;

(3) GUIDELINE C: Foreign preference;

(4) GUIDELINE D: Sexual behavior;

(5) GUIDELINE E: Personal conduct;

(6) GUIDELINE F: Financial considerations;

(7) GUIDELINE G: Alcohol consumption;

(8) GUIDELINE H: Drug involvement;

(9) GUIDELINE I: Emotional, mental, and personality disorders;

(10) GUIDELINE J: Criminal conduct;

(11) GUIDELINE K: Security violations;

(12) GUIDELINE L: Outside activities;

(13) GUIDELINE M: Misuse of Information Technology Systems.

d. 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 or questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative

agency in the face of reliable, significant, disqualifying, adverse information.

e. 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:

(1) Voluntarily reported the information;

(2) Was truthful and complete in responding to questions;

(3) Sought assistance and followed professional guidance, where appropriate;

(4) Resolved or appears likely to favorably resolve the security concern;

(5) Has demonstrated positive changes in behavior and employment;

(6) Should have his or her access temporarily suspended pending final adjudication of the information.

f. If after evaluating information of security concern, 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 the future incidents of a similar nature may result in revocation of access.

Guideline A
Allegiance to the United States

3. The Concern.

An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

4. Conditions that could raise a security concern and may be disqualifying include:

a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

b. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

c. Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means;

d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

5. Conditions that could mitigate security concerns include:

a. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

b. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

c. Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

d. The person has had no recent involvement or association with such activities.

GUIDELINE B
Foreign Influence

6. The Concern.

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 not citizens of the United States or 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.

7. Conditions that could raise a security concern and may be disqualifying include:

a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

b. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

c. Relatives, cohabitants, or associates who are connected with any foreign government;

d. Failing to report, where required, associations with foreign nationals;

e. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

f. Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

8. Conditions that could mitigate security concerns include:

a. A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

b. Contacts with foreign citizens are the result of official United States Government business;

c. Contact and correspondence with foreign citizens are casual and infrequent;

d. The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;

e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

GUIDELINE C
Foreign Preference

9. The Concern.

When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

10. Conditions that could raise a security concern and may be disqualifying include:

a. The exercise of dual citizenship;

b. Possession and/or use of a foreign passport;

c. Military service or a willingness to bear arms for a foreign country;

d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

e. Residence in a foreign country to meet citizenship requirements;

f. Using foreign citizenship to protect financial or business interests in another country;

g. Seeking or holding political office in the foreign country;

h. Voting in foreign elections; and

i. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

11. Conditions that could mitigate security concerns include:

a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

c. Activity is sanctioned by the United States;

d. Individual has expressed a willingness to renounce dual citizenship.

GUIDELINE D
Sexual Behavior

12. The Concern.

Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may

subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion.[4] Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

13. Conditions that could raise a security concern and may be disqualifying include:

a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destruction or high-risk behavior or that which is symptomatic of a personality disorder;

c. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

d. Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

14. Conditions that could mitigate security concerns include:

a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

d. The behavior no longer serves as a basis for coercion, exploitation, or duress.

GUIDELINE E
Personal Conduct

15. The Concern.

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

---

[4] The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.

a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

b. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

16. Conditions that could raise a security concern and may be disqualifying also include:

a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

b. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

d. Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

e. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;

f. Association with persons involved in criminal activity.

17. Conditions that could mitigate security concerns include:

a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

c. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

g. Association with persons involved in criminal activities has ceased.

GUIDELINE F
Financial Considerations

18. The Concern.

An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

19. Conditions that could raise a security concern and may be disqualifying include:

a. A history of not meeting financial obligations;

b. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

c. Inability or unwillingness to satisfy debts;

d. Unexplained affluence;

e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

20. Conditions that could mitigate security concerns include:

a. The behavior was not recent;

b. It was an isolated incident;

c. The conditions that resulted in the behavior were

largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);

d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

e. The affluence resulted from a legal source; and

f. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

GUIDELINE G
Alcohol Consumption

21. The Concern.

Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

22. Conditions that could raise a security concern and may be disqualifying include:

a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

d. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

e. Habitual or binge consumption of alcohol to the point of impaired judgment;

f. Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

23. Conditions that could mitigate security concerns include:

a. The alcohol-related incidents do not indicate a pattern;

b. The problem occurred a number of years ago and there is no indication of a recent problem;

c. Positive changes in behavior supportive of sobriety;

d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participated frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

GUIDELINE H
Drug Involvement

24. The Concern.

a. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

b. Drugs are defined as mood and behavior altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) Inhalants and other similar substances.

c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

25. Conditions that could raise a security concern and may be disqualifying include:

a. Any drug abuse (see above definition);

b. Illegal drug possession, including cultivation; processing, manufacture, purchase, sale, or distribution;

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

d. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

e. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

26. Conditions that could mitigate security concerns include:

a. The drug involvement was not recent;

b. The drug involvement was an isolated or aberrational event;

c. A demonstrated intent not to abuse any drugs in the future;

d. Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

GUIDELINE I
Emotional, Mental, and Personality Disorders

27. The Concern.

Emotional, mental, and personality disorders 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. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the U.S. Government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

28. Conditions that could raise a security concern and may be disqualifying include:

a. An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

c. A pattern of high-risk, irresponsible, aggressive, anti-social, or emotionally unstable behavior;

d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

29. Conditions that could mitigate security concerns include:

a. There is no indication of a current problem;

b. Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission and has a low probability of recurrence or exacerbation;

c. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

GUIDELINE J
Criminal Conduct

30. The Concern.

A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

31. Conditions that could raise a security concern and may be disqualifying include:

a. Allegations or admissions of criminal conduct, regardless or whether the person was formally charged;

b. A single serious crime or multiple lesser offenses.

32. Conditions that could mitigate security concerns include:

a. The criminal behavior was not recent;

b. The crime was an isolated incident;

c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

e. Acquittal;

f. There is clear evidence of successful rehabilitation.

GUIDELINE K
Security Violations

33. The Concern.

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

34. Conditions that could raise a security concern and may be disqualifying include:

a. Unauthorized disclosure of classified information;

b. Violations that are deliberate or multiple or due to negligence.

35. Conditions that could mitigate security concerns include actions that:

a. Were inadvertent;

b. Were isolated or infrequent;

c. Were due to improper or inadequate training;

d. Demonstrate a positive attitude towards the discharge of security responsibilities.

GUIDELINE L
Outside Activities

36. The Concern.

Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

37. Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:

a. A foreign country;

b. Any foreign national;

c. A representative of any foreign interest;

d. Any foreign, domestic, or international organization or

person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

38. Conditions that could mitigate security concerns include:

a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

GUIDELINE M
Misuse of Information Technology Systems

39. The Concern.

Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

40. Conditions that could raise a security concern and may be disqualifying include:

a. Illegal or unauthorized entry into any information technology system;

b. Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;

c. Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

d. Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

41. Conditions that could mitigate security concerns include:

a. The misuse was not recent or significant;

b. The conduct was unintentional or inadvertent;

c. The introduction or removal of media was authorized;

d. The misuse was an isolated event;

e. The misuse was followed by a prompt, good faith effort to correct the situation.

ANNEX D

Appeals Procedures: Denial or Revocation of Access

1. Policy.

This annex establishes common appeals procedures for the denial or revocation of access to sensitive compartmented information (SCI) by entities of the Intelligence Community after adjudication pursuant to the provisions of DCID 6/4. This annex is promulgated pursuant to Executive Order 12333, Executive Order 12968, and the National Security Act of 1947, as amended. For the purposes of this annex, all references to DCID 6/4 include the basic document and all of its annexes. Any individual who has been considered for initial or continued access to SCI pursuant to the provisions of DCID 6/4 shall, to the extent provided below, be afforded an opportunity to appeal the denial or revocation of such access. This annex supersedes any and all other practices and procedures for the appeal of the denial or revocation of SCI access. This annex will not be construed to require the disclosure of classified information or information concerning intelligence sources and methods, nor will it be construed to afford an opportunity to appeal before the actual denial or revocation of SCI access. In addition, the provisions of DCID 6/4, or any other document or provision of law, will not be construed to create a liberty or property interest of any kind in the access of any individual to SCI.

2. Applicability.

This annex applies to all US Government civilian and military personnel, as well as any other individuals, including contractors and employees of contractors, who are considered for initial or continued access to SCI. This annex does not apply to decisions regarding employment and will not be construed to affect or impair public Law 88-290 or the authority of any entity to effect applicant or personnel actions pursuant to Public Law 88-290, Public Law 86-36, or other applicable law.

3. SCI Access Determination Authority.

Adjudications for access to SCI will be made in accordance with DCID 6/4 by a Determination Authority designated by the Senior Official of the Intelligence Community (SOIC) of each entity. Access to SCI shall be denied or revoked whenever it is determined that a person does not meet the security standards provided for in DCID 6/4. Any doubt about an individual's eligibility for access or continued access to SCI shall be resolved in favor of the national security and access will be denied or revoked.

4. Procedures.

a. Individuals will be:

(1) Provided as comprehensive and detailed a written explanation of the basis for that determination as the national security interests of the United States and other applicable law permit.

(2) Informed in this written explanation of their right to be represented by counsel or other representative at their own expense; to request any documents, records or reports upon which a denial or revocation is based; and, to request the entire investigative file as permitted by the national security and other applicable law.

(3) Provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (5 U.S.C. 552a), as applicable, any documents, records and reports upon which a denial or revocation is based.

(4) Provided an opportunity to reply in writing within 45 days of receipt of relevant documentation to request a review of the determination.

(5) Provided written notice of and reasons for the results of the review, the identity of the deciding authority in accordance with operational requirements, and written notice of the right to appeal.

(6) Provided an opportunity to appeal in writing to a high level panel, appointed by the SOIC, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final, except when the SOIC chooses to exercise the appeal authority personally, based on a recommendation from the panel, and provided to the individual.

(7) Provided an opportunity to appear personally and to present relevant documents, materials and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the SOIC. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection a.(6) of this section, in which case the written decision of the panel shall be made part of the applicant's or employee's security record.

b. When a SOIC or their principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national

security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

c. Nothing in this annex shall prohibit a SOIC from personally exercising the appeal authority in paragraph a.(6) above based upon recommendations from an appeals panel. In such case, the decision of the SOIC shall be final.

d. A SOIC may determine that the appeal procedures prescribed in this annex cannot be invoked in a manner that is consistent with the national security. In such cases, a SOIC may deny an individual an appeal pursuant to this annex and the authority delegated to the SOIC by the DCI under the National Security Act of 1947, as amended. The SOIC's determination in this regard shall be conclusive.

e. The DCI or DDCI may take any actions regarding an individual's SCI access without regard to any of the provisions of this or any other regulation or directive. The DCI or DDCI may consult with the agency head pertaining to any action to be taken regarding an individual's SCI access.

f. This annex does not create nor confer on any person or entity any right to administrative or judicial review of these procedures, their implementation, or decisions or actions rendered thereunder. It also does not create or confer any right, benefit, or privilege, whether substantive or procedural, for access to classified information. Finally, this annex does not create or confer any substantive or procedural right, benefit, or privilege enforceable by any party against the United States or any agency, department, or instrumentality of the executive branch, its officers or employees, for any other person.

ANNEX E

Standards for SCI Security Awareness Programs in the US Intelligence Community

Consistent with controls and procedures set forth in DCID 1/19, "Security Policy for Sensitive Compartmented Information," and its supplement, "DCID 1/19 Security Policy Manual," standards are hereby established for the SCI security education programs designed to enhance the security awareness of the US Government civilian and military personnel and private contractors working in the US Intelligence Community. Compliance with these standards is required for all departments/agencies within the Intelligence Community. Existing security awareness programs will be modified to conform with these standards. Departments/agencies will establish a documented program to ensure that training has been presented to all personnel.

All individuals nominated for or holding SCI access approval will be notified initially and annually thereafter of their responsibility to report to their cognizant security officers any activities or conduct such as described in Annex C that could conflict with their ability to protect classified information from unauthorized disclosure. Any outside employment, activities or conduct that could create real or apparent conflicts with their responsibility to protect classified information must be reported.

The security awareness requirements set forth herein are divided into three phases. Phase 1 concerns the initial indoctrination of individuals, which is normally administered before access to SCI. Phase 2 concerns the continuing security awareness program required to maintain an increased security awareness throughout the period of access. Phase 3 sets forth the final guidelines and instructions when access to SCI is terminated.

1. Initial Indoctrination.

As soon as practicable after being approved for access to SCI, personnel will receive an initial security indoctrination that will include:

a. The need for and purpose of SCI, and the adverse effect on the national security that could result from unauthorized disclosure.

b. The intelligence mission of the department/agency to include the reasons why intelligence information is sensitive.

c. The administrative, personnel, physical, and other procedural security requirements of the department/agency and those requirements peculiar to specific duty assignments,

including information on who to consult to determine if particular outside employment or activity might be of concern.

d. Individual classification management responsibilities as set forth in appropriate directives and regulations to include classification/declassification guidelines and marking requirements.

e. The definitions and criminal penalties for espionage, including harboring or concealing persons; gathering, transmitting, or losing defense information; gathering or delivering defense information to aid foreign governments; photographing and sketching defense installations; unauthorized disclosure of classified information (Title 18, U.S.C., Sections 792 through 795, 797, and 798), the Internal Security Act of 1950 (Title 50, U.S.C., Section 783), the Intelligence Identities Protection Act of 1982 (Title 50, U.S.C., Sections 421 through 426) and, when appropriate, the Atomic Energy Act (Sections 224 through 227).

f. The administrative sanctions for violation or disregard for security procedures.

g. A review of the techniques employed by foreign intelligence organizations in attempting to obtain national security information.

h. Individual security responsibilities including:

(1) The prohibition against discussing SCI in a non-secure area, over a non-secure telephone, or in any other manner that permits access by unauthorized persons.

(2) The need to determine, before disseminating SCI, that the prospective recipient has the proper security access approval, that the SCI is needed in order to perform official duties, and that the recipient can properly protect the information.

(3) The need to exercise security in activities as members of professional, commercial, scholarly or advocacy organizations that publish or discuss information on intelligence, defense or foreign affairs.

(4) The continuing obligation to submit for review any planned articles, books, speeches or public statements that contain or purport to contain SCI or information relating to or derived from SCI, as specified by the nondisclosure agreements that are a prerequisite for access to SCI.

(5) Obligation to report travel to or connections with countries with aggressive proactive intelligence capabilities, or contacts with foreign nationals under certain circumstances, or

attempts (including blackmail, coercion and harassment) by unauthorized persons to obtain national security information, physical security deficiencies, and loss or possible compromise of SCI material.

(6) Obligation to report to proper authorities all activities or conduct of an individual who has access to SCI which relates to guidelines described in Annex C, such as:

(a) Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the United States Government by unconstitutional means.

(b) Foreign influence concerns/close personal association with foreign nationals.

(c) Foreign citizenship or foreign monetary interests.

(d) Sexual behavior that is criminal or reflects a lack of judgment or discretion.

(e) Unwillingness to comply with rules and regulations or to cooperate with security processing.

(f) Unexplained affluence or excessive indebtedness.

(g) Alcohol abuse.

(h) Illegal or improper drug use/involvement.

(i) Apparent mental or emotional disorder(s).

(j) Criminal conduct.

(k) Noncompliance with security requirements.

(l) Engagement in outside activities which could cause a conflict of interest.

(m) Misuse of information technology systems.

(7) Identification of the elements in the department/agency to which matters of security interest are to be referred.

2. Periodic Awareness Enhancement.

Each department/agency will establish a continuing security awareness program that will provide frequent exposure of personnel to security awareness material. Implementation of a continuing

program may include live briefings, audiovisual presentations (e.g., video tapes, films, and slide/tape programs), printed material (e.g., posters, memorandums, pamphlets, fliers), or a combination thereof. It is essential that current information and materials be utilized. Programs should be designed to meet the particular needs of the department/agency.

a. The basic elements for this program will include, but are not limited to, the following:

(1) The foreign intelligence threat (including the threats associated with foreign travel and foreign associations).

(2) The technical threat.

(3) Administrative, personnel, physical, and procedural security.

(4) Individual classification management responsibility.

(5) Criminal penalties and administrative sanctions.

(6) Individual security responsibilities.

(7) A review of other appropriate department/agency requirements.

b. Special security briefings/debriefings should supplement the existing security awareness programs in the following situations:

(1) When an individual is designated as a courier.

(2) When high risk situations are present, specifically:

(a) When an individual travels, officially or unofficially, to or through countries with aggressive/proactive intelligence capabilities or with connection(s) to terrorism or criminal activity, or:

(b) When an individual has, or anticipates contact with a representative(s) of the countries identified above.

(3) When any other situation arises for which the SOIC or designee determines that an increased level of protection is necessary.

3. Debriefing.

When a department/agency has determined that access to SCI is no longer required, final instructions and guidelines will be provided to the individual. At a minimum these shall include:

a. A requirement that the individual read appropriate sections of Titles 18 and 50, U.S.C., and that the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure be clarified.

b. The continuing obligation, under the prepublication and other provisions of the nondisclosure agreement for SCI, never to divulge; publish; or reveal by writing, word, conduct, or otherwise, to any unauthorized persons any SCI, without the written consent of appropriate department/agency officials.

c. An acknowledgment that the individual will report without delay to the Federal Bureau of Investigation, or the department/agency, any attempt by an unauthorized person to solicit national security information.

d. A declaration that the individual no longer possesses any documents or material containing SCI.

e. A reminder of the risks associated with foreign travel and foreign association.

ANNEX F[5]

Reciprocity of SCI Eligibility Determinations

1. Reciprocity Policy.

a. Within the Intelligence Community, subject to the conditions set forth below, a favorable DCID 6/4 eligibility determination for access to SCI made by one adjudicative authority under SOIC cognizance is a favorable determination for all SOICs. Reciprocity of eligibility determinations does not in itself constitute reciprocity of need-to-know determinations. Need-to-know determinations are always distinct and separate decisions.

b. Reciprocity requires adjudication by trained government adjudicators under SOIC cognizance and a system for monitoring continuing security eligibility. Eligibility decisions, including the presence of exceptions, must be a matter of record accessible to the Intelligence Community's access granting authorities.

c. DCID 6/4 eligibility determinations are mutually acceptable and will not be readjudicated if:

(1) They are made without exception, and

(2) No substantial issue information exists since the most recent adjudication, and

(3) The appropriate type of polygraph examination, if one is required, has been satisfactorily completed.

d. Agencies may accept or reject DCID 6/4 eligibility determinations where exceptions exist based upon their own assessment of risk. Any agency rejecting another's determination of eligibility where exceptions exist will notify, to the extent it is able to do so, all adjudicative authorities having an eligibility interest in the person of its decision. Those authorities, in turn, may reassess the appropriateness of continuing to hold the person eligible with an exception.

e. Where an agency or organization has additional but not duplicative requirements, the actual granting of access is contingent upon satisfying those requirements. Failure to meet an additional but not duplicative requirement may not necessarily adversely affect a person's continued eligibility for reciprocal access with other organizations and agencies. However, the agency that made the original eligibility determination may use new information obtained by another organization to readjudicate the

[5] Annex F was signed by the DCI on 13 Oct 99. At that time, the number of DCID 1/14 was changed to 6/4 to correspond to an appropriate section in DCID 1/1

person's continued eligibility subject to restrictions placed on use of the information by the organization that obtained it.

f. A person determined ineligible for SCI access will remain ineligible for a minimum of one year. However, SOICs or their designees may waive this requirement in individual cases based on operational necessity and an assessment by the relevant determination authority that there is no unacceptable security risk in doing so.

g. This annex does not apply to suitability decisions for employment.

2. Definitions.

a. *Exception*: An adjudicative decision to grant or continue access eligibility despite a failure to meet adjudicative or investigative standards. Regarding SCI access eligibility, only the DCI or, as appropriate, the concerned Senior Official of the Intelligence Community (SOIC) or designee will make such decisions. An exception precludes reciprocity without review of the case by the gaining organization or program. There are three types:

(1) *Condition*: Access eligibility granted or continued with the proviso that one or more additional measures will be required. Such measures include additional security monitoring, restrictions on access, and restrictions on the individual's handling of classified information. Submission of periodic financial statements, admonishment regarding use of drugs or excessive use of alcohol, and satisfactory progress in a government-approved counseling program are examples of conditions.

(2) *Deviation*: Access eligibility granted or continued despite either a significant gap in coverage or scope in the investigation or an out-of-date investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of six months or more within the most recent five years investigated or the lack of an FBI name check or technical check or the lack of one or more relevant investigative scope components (e.g., employment checks or a subject interview for an SSBI, financial review for any investigation) in its entirety.

(3) *Waiver*: Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. The DCI, SOIC, or SOIC's designee approve waivers pursuant to their authorities outlined in DCID 6/4, paragraphs 6a and b, only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require special limitations on access, additional security monitoring and other restrictions on the person's handling of classified information beyond normal need-to-know. Paragraph 6 of DCID 6/4 governs the granting of waivers insofar as

they pertain to SCI access eligibility. In the Intelligence Community, waivers may be contemplated when the person under consideration for SCI access is not a United States citizen, when any member of that person's immediate family is not a US citizen, or when any member of the immediate family or other person with whom there is a bond of affection or obligation is subject to duress.

b. *Issue information*: Any information that could adversely affect a person's eligibility for access to classified information. There are two types:

(1) *Minor issue information*: Information that meets a threshold of concern set out in "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" (see Annex C to DCID 6/4), but for which adjudication determines that adequate mitigation, as provided for by the Guidelines, exists. Minor issue information does not provide the basis for a waiver or condition.

(2) *Substantial issue information*: Any information, or aggregate of information, that raises a significant question about the prudence of granting access eligibility. Substantial issue information constitutes the basis for granting access eligibility with waiver or condition, or for denying or revoking access eligibility. Granting access eligibility when substantial issue information exists is predicated upon meeting the requirements of paragraphs 12a and b of DCID 6/4 for tailored security programs whose purpose is to resolve issues.

c. *Need to know*: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

d. *Reciprocity*: Acceptance by one SOIC of an SCI access eligibility determination made by another. It applies both to granting access when another SOIC has approved and denying access when another SOIC has denied or revoked. Reciprocity does not include agency determinations of employment suitability. Nothing precludes SOICs or their designees from exercising authority to grant or to deny access for reasons of operational necessity regardless of another SOIC's decision.

3. The Effect of the Polygraph on Reciprocity.

The Intelligence Community uses the polygraph in defined circumstances to provide additional information to the adjudicative process. Reciprocity of an SCI eligibility determination when a polygraph requirement exists is conditional upon satisfactory completion of that requirement.

4. Review of Access Determinations.

All denials or revocations of access eligibility are subject to the review proceedings outlined in Annex D, above.

Appendix D

Defense Office of Hearings and Appeals, Additional Procedural Guidance

DEFENSE OFFICE OF HEARINGS AND APPEALS

ADDITIONAL PROCEDURAL GUIDANCE

1. When the DISCO cannot affirmatively find that it is clearly consistent with the national interest to grant or continue a security clearance for an applicant, the case shall be promptly referred to the DISCR.

2. Upon referral, the DISCR shall make a prompt determination whether to grant or continue a security clearance, issue a statement of reasons (SOR) as to why it is not clearly consistent with the national interest to do so, or take interim actions, including but not limited to:

a. Direct further investigation.

b. Propound written interrogatories to the applicant or other persons with relevant information.

c. Requiring the applicant to undergo a medical evaluation by a DoD Psychiatric Consultant.

d. Interviewing the applicant.

3. An unfavorable clearance decision shall not be made unless the applicant has been provided with a written SOR that shall be as detailed and comprehensive as the national security permits. A letter of instruction with the SOR shall explain that the applicant or Department Counsel may request a hearing. It shall also explain the adverse consequences for failure to respond to the SOR within the prescribed time frame.

4. The applicant must submit a detailed written answer to the SOR under oath or affirmation that shall admit or deny each listed allegation. A general denial or other similar answer is insufficient. To be entitled to a hearing, the applicant must specifically request a hearing in his or her answer. The answer must be received by the DISCR within 20 days from receipt of the SOR. Requests for an extension of time to file an answer may be submitted to the Director, DISCR, or designee, who in turn may grant the extension only upon a showing of good cause.

5. If the applicant does not file a timely and responsive answer to the SOR, the Director, DISCR, or designee, may discontinue processing the case, deny issuance of the requested

security clearance, and direct the DISCO to revoke any security clearance held by the applicant.

6. Should review of the applicant's answer to the SOR indicate that allegations are unfounded, or evidence is insufficient for further processing, Department Counsel shall take such action as appropriate under the circumstances, including but not limited to withdrawal of the SOR and transmittal to the Director for notification of the DISCO for appropriate action.

7. If the applicant has not requested a hearing with his or her answer to the SOR and Department Counsel has not requested a hearing within 20 days of receipt of the applicant's answer, the case shall be assigned to an Administrative Judge for a clearance decision based on the written record. Department Counsel shall provide the applicant with a copy of all relevant and material information that could be adduced at a hearing. The applicant shall have 30 days from receipt of the information in which to submit a documentary response setting forth objections, rebuttal, extenuation, mitigation, or explanation, as appropriate.

8. If a hearing is requested by the applicant or Department Counsel, the case shall be assigned to an Administrative Judge for a clearance decision based on the hearing record. Following issuance of a notice of hearing by the Administrative Judge, or designee, the applicant shall appear in person with or without counsel or a personal representative at a time and place designated by the notice of hearing. The applicant shall have a reasonable time to prepare his or her case. The applicant shall be notified at least 15 days in advance of the time and place of the hearing, which generally shall be held at a location in the United States within a metropolitan area near the applicant's place of employment or residence. A continuance may be granted by the Administrative Judge only for good cause. Hearings may be held outside of the United States in NATO cases, or in other cases upon a finding of good cause by the Director, DISCR, or designee.

9. The Administrative Judge may require a prehearing conference.

10. The Administrative Judge may rule on questions on procedure, discovery, and evidence and shall conduct all proceedings in a fair, timely, and orderly manner.

11. Discovery by the applicant is limited to non-privileged documents and materials subject to control by the DISCR. Discovery by Department Counsel after issuance of an SOR may be granted by the Administrative Judge only upon a showing of good cause.

12. A hearing shall be open except when the applicant requests that it be closed, or when the Administrative Judge determines that there is a need to protect classified information or there is other good cause for keeping the proceeding closed. No inference shall be drawn as to the merits of a case on the basis of a request that the hearing be closed.

13. As far in advance as practical, Department Counsel and the applicant shall serve one another with a copy of any pleading, proposed documentary evidence, or other written communication to be submitted to the Administrative Judge.

14. Department Counsel is responsible for presenting witnesses and other evidence to establish facts alleged in the SOR that have been controverted.

15. The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision.

16. Witnesses shall be subject to cross-examination.

17. The SOR may be amended at the hearing by the Administrative Judge on his or her own motion, or upon motion by Department Counsel or the applicant, so as to render it in conformity with the evidence admitted or for other good cause. When such amendments are made, the Administrative Judge may grant either party's request for such additional time as the Administrative Judge may deem appropriate for further preparation or other good cause.

18. The Administrative Judge hearing the case shall notify the applicant and all witnesses testifying that 18 U.S.C. 1001 (reference (c)) is applicable.

19. The Federal Rules of Evidence (28 U.S.C. 101 et seq. (reference (d))) shall serve as a guide. Relevant and material evidence may be received subject to rebuttal, and technical rules

of evidence may be relaxed, except as otherwise provided herein, to permit the development of a full and complete record.

20. Official records or evidence compiled or created in the regular course of business, other than DoD personnel background reports of investigation (ROI), may be received and considered by the Administrative Judge without authenticating witnesses, provided that such information has been furnished by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary of Defense, or the Department or Agency head concerned, to safeguard classified information within industry under E.O. 10865 (enclosure 1). An ROI may be received with an authenticating witness provided it is otherwise admissible under the Federal Rules of Evidence (28 U.S.C. 101 et seq. (reference (d))).

21. Records that cannot be inspected by the applicant because they are classified may be received and considered by the Administrative Judge, provided the GC, DoD, has:

a. Made a preliminary determination that such evidence appears to be relevant and material.

b. Determined that failure to receive and consider such evidence would be substantially harmful to the national security.

22. A written or oral statement adverse to the applicant on a controverted issue may be received and considered by the Administrative Judge without affording an opportunity to cross-examine the person making the statement orally, or in writing when justified by the circumstances, only in either of the following circumstances:

a. If the head of the Department or Agency supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his or her identity would be substantially harmful to the national interest; or

b. If the GC, DoD, has determined the statement concerned appears to be relevant, material, and reliable; failure to receive and consider the statement would be substantially harmful to the national security; and the person who furnished the information cannot appear to testify due to the following:

(1) Death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant; or

(2) Some other cause determined by the Secretary of Defense, or when appropriate by the Department or Agency head, to be good and sufficient.

23. Whenever evidence is received under items 21. or 22., above, the applicant shall be furnished with as comprehensive and detailed a summary of the information as the national security permits. The Administrative Judge and Appeal Board may make a clearance decision either favorable or unfavorable to the applicant based on such evidence after giving appropriate consideration to the fact that the applicant did not have an opportunity to confront such evidence, but any final determination adverse to the applicant shall be made only by the Secretary of Defense, or the Department or Agency head, based on a personal review of the case record.

24. A verbatim transcript shall be made of the hearing. The applicant shall be furnished one copy of the transcript, less the exhibits, without cost.

25. The Administrative Judge shall make a written clearance decision in a timely manner setting forth pertinent findings of fact, policies, and conclusions as to the allegations in the SOR, and whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant. The applicant and Department Counsel shall each be provided a copy of the clearance decision. In cases in which evidence is received under items 21. and 22., above, the Administrative Judge's written clearance decision may require deletions in the interest of national security.

26. If the Administrative Judge decides that it is clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the DISCO shall be so notified by the Director, DISCR, or designee, when the clearance decision becomes final in accordance with item 36., below.

27. If the Administrative Judge decides that it is not clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the Director, DISCR, or designee, shall expeditiously notify the DISCO, which shall in turn notify the applicant's employer of the denial or

revocation of the applicant's security clearance. The letter forwarding the Administrative Judge's clearance decision to the applicant shall advise the applicant that these actions are being taken, and that the applicant may appeal the Administrative Judge's clearance decision.

28. The applicant or Department Counsel may appeal the Administrative Judge's clearance decision by filing a written notice of appeal with the Appeal Board within 15 days after the date of the Administrative Judge's clearance decision. A notice of appeal received after 15 days from the date of the clearance decision shall not be accepted by the Appeal Board, or designated Board Member, except for good cause. A notice of cross appeal may be filed with the Appeal Board within 10 days of receipt of the notice of appeal. An untimely cross appeal shall not be accepted by the Appeal Board, or designated Board Member, except for good cause.

29. Upon receipt of a notice of appeal, the Appeal Board shall be provided the case record. No new evidence shall be received or considered by the Appeal Board.

30. After filing a timely notice of appeal, a written appeal brief must be received by the Appeal Board within 45 days from the date of the Administrative Judge's clearance decision. The appeal brief must state the specific issue or issues being raised, and cite specific portions of the case record supporting any alleged error. A written reply brief, if any, must be filed within 20 days from receipt of the appeal brief. A copy of any brief filed must be served upon the applicant or Department Counsel, as appropriate.

31. Requests for extension of time for submission of briefs may be submitted to the Appeal Board or designated Board Member. A copy of any request for extension of time must be served on the opposing party at the time of submission. The Appeal Board, or designated Board Member, shall be responsible for controlling the Appeal Board's docket, and may enter an order dismissing an appeal in an appropriate case or vacate such an order upon a showing of good cause.

32. The Appeal Board shall address the material issues raised by the parties to determine whether harmful error occurred. Its scope of review shall be to determine whether or not:

a. The Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record. In making this review, the Appeal Board shall give deference to the credibility determinations of the Administrative Judge;

b. The Administrative Judge adhered to the procedures required by E.O. 10865 (enclosure 1) and this Directive; or

c. The Administrative Judge's rulings or conclusions are arbitrary, capricious, or contrary to law.

33. The Appeal Board shall issue a written clearance decision addressing the material issues raised on appeal. The Appeal Board shall have authority to:

a. Affirm the decision of the Administrative Judge;

b. Remand the case to an Administrative Judge to correct identified error. If the case is remanded, the Appeal Board shall specify the action to be taken on remand; or

c. Reverse the decision of the Administrative Judge if correction of identified error mandates such action.

34. A copy of the Appeal Board's written clearance decision shall be provided to the parties. In cases in which evidence was received under items 21. and 22., above, the Appeal Board's clearance decision may require deletions in the interest of national security.

35. Upon remand, the case file shall be assigned to an Administrative Judge for correction of error(s) in accordance with the Appeal Board's clearance decision. The assigned Administrative Judge shall make a new clearance decision in the case after correcting the error(s) identified by the Appeal Board. The Administrative Judge's clearance decision after remand shall be provided to the parties. The clearance decision after remand may be appealed pursuant to items 28. to 35., above.

36. A clearance decision shall be considered final when:

a. A security clearance is granted or continued pursuant to item 2., above;

b. No timely notice of appeal is filed;

c. No timely appeal brief is filed after a notice of appeal has been filed;

d. The appeal has been withdrawn;

e. When the Appeal Board affirms or reverses an Administrative Judge's clearance decision; or

f. When a decision has been made by the Secretary of Defense, or the Department or Agency head, under to item 23., above.

The Director, DISCR, or designee, shall notify the DISCO of all final clearance decisions.

37. An applicant whose security clearance has been finally denied or revoked by the DISCR is barred from reapplication for 1 year from the date of the initial unfavorable clearance decision.

38. A reapplication for a security clearance must be made initially by the applicant's employer to the DISCO and is subject to the same processing requirements as those for a new security clearance application. The applicant shall thereafter be advised he is responsible for providing the Director, DISCR, with a copy of any adverse clearance decision together with evidence that circumstances or conditions previously found against the applicant have been rectified or sufficiently mitigated to warrant reconsideration.

39. If the Director, DISCR, determines that reconsideration is warranted, the case shall be subject to this Directive for making a clearance decision.

40. If the Director, DISCR, determines that reconsideration is not warranted, the DISCR shall notify the applicant of this decision. Such a decision is final and bars further reapplication for an additional one year period from the date of the decision rejecting the reapplication.

41. Nothing in this Directive is intended to give an applicant reapplying for a security clearance any greater rights than those applicable to any other applicant under this Directive.

42.. An applicant may file a written petition, under oath or affirmation, for reimbursement of loss of earnings resulting from the suspension, revocation, or denial of his or her security clearance. The petition for reimbursement must include as an attachment the favorable clearance decision and documentation supporting the reimbursement claim. The Director, DISCR, or designee, may in his or her discretion require additional information from the petitioner.

43. Claims for reimbursement must be filed with the Director, DISCR, or designee, within 1 year after the date the security clearance is granted. Department Counsel generally shall file a response within 60 days after receipt of applicant's petition for reimbursement and provide a copy thereof to the applicant.

44. Reimbursement is authorized only if the applicant demonstrates by clear and convincing evidence to the Director, DISCR, that all of the following conditions are met:

a. The suspension, denial, or revocation was the primary cause of the claimed pecuniary loss; and

b. The suspension, denial, or revocation was due to gross negligence of the Department of Defense at the time the action was taken, and not in any way by the applicant's failure or refusal to cooperate.

45. The amount of reimbursement shall not exceed the difference between the earnings of the applicant at the time of the suspension, revocation, or denial and the applicant's interim earnings, and further shall be subject to reasonable efforts on the part of the applicant to mitigate any loss of earnings. No reimbursement shall be allowed for any period of undue delay resulting from the applicant's acts or failure to act. Reimbursement is not authorized for loss of merit raises and general increases, loss of employment opportunities, counsel's fees, or other costs relating to proceedings under this Directive.

46. Claims approved by the Director, DISCR, shall be forwarded to the Department or Agency concerned for payment. Any payment made in response to a claim for reimbursement shall be in full satisfaction of any further claim against the United States or any Federal Department or Agency, or any of its officers or employees.

47. Clearance decisions issued by Administrative Judges and the Appeal Board shall be indexed and made available in redacted form to the public.

Appendix E

Defense Office of Hearings and Appeals, Memorandum for all Applicants and Their Respective Attorneys or Personal Representatives, and Department Counsel, Prehearing Guidance for DOHA Hearings

DEPARTMENT OF DEFENSE
DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS
WASHINGTON HEARING OFFICE
POST OFFICE BOX 3627
ARLINGTON, VIRGINIA 22203
(703) 696-4542

MEMORANDUM FOR ALL APPLICANTS AND THEIR RESPECTIVE ATTORNEYS OR PERSONAL REPRESENTATIVES, AND DEPARTMENT COUNSEL

SUBJECT: Prehearing Guidance for DOHA[1] hearings

In an effort to expedite the hearing in DOHA industrial security clearance cases, the following guidance is being sent to Applicants and their respective attorneys or Personal Representatives, and Department Counsel (the parties) to assist them in preparing for the hearing. This guidance is not exhaustive, and the parties should also refer to Department of Defense Directive 5220.6 for guidance on hearing matters. In the event of any conflict between this guidance and the provisions of DoD Directive 5220.6,[2] the provisions of the Directive control.

1. The hearing is an adversarial proceeding in which the parties have the responsibility to present their respective cases. The Government is normally represented by an attorney known as a Department Counsel. The Applicant has the option of appearing by himself or herself without an attorney, or being represented by an attorney selected and paid for by the Applicant, or by being represented by a Personal Representative such as a friend, family member, or union representative.

2. Each party is expected to be prepared to present at the hearing whatever evidence (testimonial or documentary, or both) that party intends to offer. In this regard, it should be noted that the Administrative Judge is not empowered by law to issue a subpoena. Thus, the appearance of witnesses or production of documents is purely voluntary.

3. To facilitate the exchange of correspondence, proposed evidence, the handling of preliminary matters, and the scheduling of hearings, any person representing an Applicant should file a written Entry or Notice of Appearance with both Department Counsel and the Hearing Office Docket Clerk. No special form or format is required.

4. A party requesting a continuance of a scheduled hearing date must make a *timely showing of good cause, **in writing***, for any such continuance. Among the factors to be considered are the

---

[1]The Directorate for Industrial Security Clearance Review (DISCR) was redesignated as the Defense Office of Hearings and Appeals (DOHA), effective May 20, 1994.

[2]The January 2, 1992 edition of the Directive has been amended on three occasions: Change 1 became effective on November 22, 1993; Change 2 became effective on May 20, 1994; and Change 3 became effective on February 16, 1996.

requester's diligence in readying his or her case prior to the date set for the hearing, and inconvenience to the opposing party, witnesses, and the Administrative Judge. Failure of an Applicant to appear for the scheduled hearing or to comply with an order of the Administrative Judge may result in the case being returned to the Director, DOHA for discontinuance of processing and revocation of any security clearance the Applicant currently possesses.

5. Neither party should attempt to furnish any information relating to the case without giving the other party the opportunity to be present. Such actions constitute what are known as prohibited *ex parte* communications. Also, copies of any proposed exhibits must not be submitted to the Administrative Judge prior to the hearing. Any documents to be offered as evidence should be presented at the hearing itself during the presentation of that party's case. In some instances, when an Applicant has appended documents to the response to the Statement of Reasons, the documents have been returned with an explanation that such materials are inappropriate to a pleading and that they should be resubmitted as proposed exhibits during the hearing. If such action has occurred, an Applicant should inform the Administrative Judge during the hearing, and be prepared to again offer the material previously rejected.

6. The order of proceeding is as follows: Department Counsel may make an opening statement. Then, Applicant may make an opening statement,[3] waive opening statement, or wait until the Government has concluded calling witnesses and submitting evidence before making or waiving his or her opening statement. The Government presents its case (testimony of witnesses or presentation of documents, or both) first, followed by the Applicant's case. The parties will have the opportunity to present rebuttal evidence as appropriate.

7. The parties have a wide degree of discretion in deciding what order to present the evidence in their respective cases. The Federal Rules of Evidence are used as a guide.

8. The parties should *not* mark any proposed exhibits. At the hearing, the Administrative Judge will mark the exhibits. Exhibits offered as evidence, but not admitted as such, will be retained by the Administrative Judge. As a general rule, photocopies of documents may be offered in lieu of the original, *provided* that the copies are legible. In the case of public records or business records, it is ***not*** required that the copies being offered be certified copies. However, nothing in this paragraph relieves a party from the responsibility of laying a proper foundation for a document when necessary. It is generally good practice to make sufficient photocopies of each proposed exhibit so that separate complete copies can be offered to the Administrative Judge and the opposing party. Preparation of such additional copies should take place before the scheduled hearing date, because there may not be any photocopying facilities available at the hearing location.

[3]An opening statement is not evidence. It is merely a summary of the theory of the case and a brief explanation as to the nature of the expected testimony of witnesses and the nature of documents, which serves to provide the Administrative Judge with some general idea of the case to be better able to understand the evidence.

9. Witnesses will be sequestered (kept out of the hearing room while other witnesses are testifying) during the hearing, with the exception of the Applicant and any expert witnesses. The parties may have the assistance of any expert witness, selected and paid for by the party wishing to call the witness, during the course of the hearing.

10. The Administrative Judge does not swear in Applicants or other witnesses who testify. Instead the Administrative Judge will direct their attention to, and advise them that Section 1001 of Title 18 of the United States Code applies to the proceedings. Section 1001 of Title 18 of the United States Code makes it a criminal offense, punishable by a maximum of 5 years in prison and a $10,000 fine, or both, to knowingly and willfully make a false or misleading statement or representation to any department or agency of the United States.

11. All witnesses are subject to cross-examination, or questioning, by the other party. The scope of cross-examination is not limited to the scope of the witness's direct examination. However, any cross-examination must cover issues that are material and relevant to the issues in the case or the witness's credibility. As a general rule, the parties will be allowed an opportunity to conduct one redirect examination and one recross-examination of a witness. The Administrative Judge may, in his or her discretion, question any witness.

12. Each party has the right to raise appropriate objections to any evidence, or portion thereof, being offered by the other party. Objections must be made in a timely fashion. Failure to raise an objection, at the time the objectionable evidence or testimony is offered, will be construed as acquiescence. When raising an objection, the objecting party should address the objection to the Administrative Judge, stating the basis for the objection.[4] The non-objecting party will be given an opportunity to respond to the objection, if he or she wishes. The Administrative Judge will rule on any objection raised. In the event an objection is overruled, the objecting party has an automatic exception to the Administrative Judge's ruling.

13. After completion of the presentation of evidence by the parties, they will have an opportunity to make closing arguments.[5] Department Counsel will go first. Applicant follows, with Department Counsel having a right to rebuttal. Applicant does not have a right to respond to Department Counsel's rebuttal argument.

14. A court reporter will be present to make an official transcript of the hearing. The court reporter will send the original transcript to the Administrative Judge, and a copy of the transcript, free of charge, to the Applicant or Applicant's attorney, as appropriate.

---

[4]An Applicant, not represented by an attorney, need only state the objection as clearly as he or she can, in plain English. "Legalese" is not necessary.

[5]A closing statement is not evidence. It is merely a review of the significant evidence and commentary regarding the applicability or non-applicability, as appropriate, of adjudication policy factors, both disqualifying and mitigating, as set forth in the Directive, which serves to provide the Administrative Judge with a better or "guided" understanding of the evidence.

15. The Administrative Judge will ***not*** announce his or her decision to the parties at the end of the hearing. A copy of the Administrative Judge's written decision will be sent to the parties by letter explaining the provisions for appeal.

16. The Administrative Judge has the discretion to vary the provisions of this guidance upon a showing of good cause, or whenever necessary to provide for the fair and efficient administration of the proceeding under the Directive.

Robert R. Gales
Chief Administrative Judge

Appendix F

Defense Office of Hearings and Appeals, Statement of Reasons

DEPARTMENT OF DEFENSE
DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS
POST OFFICE BOX 3656
ARLINGTON, VIRGINIA 22203-1995

In re:	)	
	)	
	)	
SSN: ____	)	ISCR Case No.
	)	
Applicant for Security Clearance	)	
	)	
	)	

STATEMENT OF REASONS

A review of your eligibility for security clearance has been made pursuant to Executive Order 10865, as amended, and as implemented by DoD Directive 5220.6, dated January 2, 1992, and this office is unable to find that it is clearly consistent with the national interest to grant you access to any classified information and recommends that your case be submitted to an Administrative Judge for a determination whether to deny or revoke your security clearance. This recommendation is based on the following reasons:

1. Criterion J: A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness. Available information raising this concern shows that:

a. You mischarged labor costs to a government contract on one occasion in 1995 when you knowingly submitted a false time card for an absent employee.

b. You mischarged labor costs to government contracts in 1995 when you distributed contract charge numbers to employees, directing them to

charge labor costs to these contracts on which they may not have directly worked.

c. You were terminated for cause from employment with , on October 17, 1995, due to violation of company rules, i.e., you mischarged labor costs to government contracts as set forth in subparagraphs 1.a., and 1.b., above.

d. That information set forth under paragraph 2., below, which constitutes a violation of Federal law, Title 18, United States Code, Section 1001, a felony.

2. Criterion E: Conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. Available information raising this concern shows:

a. In a signed, sworn statement dated September 20, 1996, and presented to a Special Agent of the Defense Investigative Service, you misrepresented material facts in that you stated you had signed off on a false entry on an employee's time card but you denied you had otherwise mischarged labor costs on government contracts; when in fact, you had also directed employees to charge labor costs to various government contracts on which they may not have worked.

b. During a March 20, 1997 interview with a Special Agent of the Defense Investigative Service, you misrepresented material facts in that you stated you had knowingly submitted a false time card for an absent employee, claiming it was an isolated incident, and denied you had otherwise mischarged labor costs at any other time, when, in fact, you had also mischarged labor costs to government contracts when you distributed contract numbers to employees directing them to charge labor to these contracts on which they may not have worked.

The criteria cited above will be found in Enclosure 2 of the referenced DoD Directive 5220.6.

Robert Karnes
Personnel Security Specialist

DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS

In re:	)	
	)	
	)	ISCR Case No.
	)	
Applicant	)	

ANSWER TO STATEMENT OF REASONS

applicant, in answer to the Statement of Reasons and in response to the specific numbered paragraphs states as follows:

1a. Denied.

1b. Denied.

1c. Denied, except that I admit my employment was terminated by on

1d. Denied.

2a. Denied.

2b. Denied.

Applicant does request a hearing.

_____

COUNTY OF _____)
)
STATE OF _____)

SUBSCRIBED AND SWORN to by before me, a Notary Public, in the jurisdiction aforesaid this _____ day of

_____
Notary Public

My Commission Expires:

DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS

In re:)
)
) ISCR Case No.
)
Applicant)

ANSWER TO STATEMENT OF REASONS

applicant, in answer to the Statement of Reasons and in response to the specific numbered paragraphs states as follows:

1a. Denied.

1b. Denied.

1c. Denied, except that I admit my employment was terminated by on

1d. Denied.

2a. Denied.

2b. Denied.

Applicant does request a hearing.

_____

COUNTY OF _____)
)
STATE OF _____)

SUBSCRIBED AND SWORN to by before me, a Notary Public, in the jurisdiction aforesaid this _____ day of

_____
Notary Public

My Commission Expires:

Appendix G

Department of Energy, Part 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material

PART 710—CRITERIA AND PROCEDURES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED MATTER OR SPECIAL NUCLEAR MATERIAL

Subpart A—General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material

GENERAL PROVISIONS

CRITERIA AND PROCEDURES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED MATTER OR SPECIAL NUCLEAR MATERIAL

ADMINISTRATIVE REVIEW

MISCELLANEOUS

ADMINISTRATIVE REVIEW

§710.20 Purpose of administrative review.

These procedures establish methods for the conduct of the administrative review of questions concerning an individual's eligibility for access authorization when it is determined that such questions cannot be favorably resolved by interview or other action.

§710.21 Notice to individual.

(a) When the Director, Office of Safeguards and Security, has authorized the institution of administrative review procedures with respect to an individual's questioned eligibility for access authorization, in accordance with §710.9, the Manager shall direct the preparation of a notification letter, approved by the local Office of Chief Counsel, or the Office of General Counsel for Headquarters cases, for delivery to the individual within 30 calendar days of the receipt of such directive from the Office of Safeguards and Security, unless an extension has been authorized by the Director, Office of Safeguards and Security. Where practicable, such letter shall be presented to the individual in person.

(b) The letter shall state:

(1) That reliable information in the possession of DOE has created a substantial doubt concerning the individual's eligibility for access authorization.

(2) The information which creates a substantial doubt regarding the individual's eligibility for access authorization (which shall be as comprehensive and detailed as the national interest permits).

(3) That the individual has the option to have the substantial doubt regarding eligibility for access authorization resolved in one of two ways:

(i) By the Manager, without a hearing, on the basis of the existing information in the case;

(ii) By personal appearance before a Hearing Officer (a "hearing").

(4) That, if the individual desires a hearing, the individual must, within 20 calendar days of the date of receipt of the notification letter, indicate this in writing to the Manager from whom the letter was received.

(5) That the individual may also file with the Manager the individual's written answer to the reported information which raises the question of the individual's eligibility for access authorization, and that, if the individual requests a hearing without filing a written answer, the request shall be deemed a general denial of all of the reported information.

(6) That, if the individual so requests, a hearing will be scheduled before a Hearing Officer, with due regard for the convenience and necessity of the parties or their representatives, for the purpose of affording the individual an opportunity of supporting his eligibility for access authorization;

(7) That, if a hearing is requested, the individual will have the right to appear personally before a Hearing Officer; to present evidence in his own behalf, through witnesses, or by documents, or both; and, subject to the limitations set forth in §710.26(g), to be present during the entire hearing and be accompanied, represented, and advised by counsel or representative of the individual's choosing and at the individual's own expense;

(8) That the individual's failure to file a timely written request for a hearing before a Hearing Officer in accordance with paragraph (b)(4) of this section, unless time deadlines are extended for good cause, will be considered as a relinquishment by the individual of the right to a hearing provided in this subpart, and that in such event a final decision will be made by the Manager; and

(9) That in any proceedings under this subpart DOE Counsel will be participating on behalf of and representing the Department of Energy, and that any statements made by the individual to DOE Counsel may be used in subsequent proceedings.

§ 710.22 Additional information.

The notification letter referenced in § 710.21 shall also:

(a) Describe the individual's access authorization status until further notice;

(b) Advise the individual of the right to counsel at the individual's own expense at each and every stage of the proceeding;

(c) Provide the name and telephone number of the designated DOE official to contact for any further information desired, including an explanation of the individual's rights under the Privacy Act of 1974; and

(d) Include a copy of 10 CFR Part 710, Subpart A.

§ 710.23 Extensions of time by the Operations Office Manager.

The Manager may, for good cause shown, at the written request of the individual, extend the time for filing a written request for a hearing, and/or the time for filing a written answer to the matters contained in the notification letter. The Manager shall notify the Director, Office of Safeguards and Security, when such extensions have been approved.

§ 710.24 Appointment of DOE Counsel.

(a) Upon receipt from the individual of a written request for a hearing, an attorney shall forthwith be assigned by the Manager to act as DOE Counsel.

(b) DOE Counsel is authorized to consult directly with the individual if he is not represented by counsel, or with the individual's counsel or representative if so represented, to clarify issues and reach stipulations with respect to testimony and contents of documents and other physical evidence. Such stipulations shall be binding upon the individual and the DOE Counsel for the purposes of this subpart.

§ 710.25 Appointment of Hearing Officer; prehearing conference; commencement of hearings.

(a) Upon receipt of a request for a hearing, the Manager shall in a timely manner transmit that request to the Office of Hearings and Appeals, and identify the DOE Counsel. The Manager shall at the same time transmit a copy of the notification letter and the individual's response to the Office of Hearings and Appeals.

(b) Upon receipt of the hearing request from the Manager, the Director, Office of Hearings and Appeals, shall appoint, as soon as practicable, a Hearing Officer.

(c) Immediately upon appointment of the Hearing Officer, the Office of Hearings and Appeals shall notify the individual and DOE Counsel of the Hearing Officer's identity and the address to which all further correspondence should be sent.

(d) The Hearing Officer shall have all powers necessary to regulate the conduct of proceedings under this subpart, including, but not limited to, establishing a list of persons to receive service of papers, issuing subpoenas for witnesses to attend the hearing or for the production of specific documents or other physical evidence, administering oaths and affirmations, ruling upon motions, receiving evidence, regulating the course of the hearing, disposing of procedural requests or similar matters, and taking other actions consistent with the regulations in this subpart. Requests for subpoenas shall be liberally granted except where the Hearing Officer finds that the grant of subpoenas would clearly result in evidence or testimony that is repetitious, incompetent, irrelevant, or immaterial to the issues in the case. The Hearing Officer may take sworn testimony, sequester witnesses, and control the dissemination or reproduction of any record or testimony taken pursuant to

this part, including correspondence, or other relevant records or tangible evidence including, but not limited to, information retained in computerized or other automated systems in possession of the subpoenaed person.

(e) The Hearing Officer will determine the day, time, and place for the hearing. Hearings will normally be held at or near the appropriate DOE facility, unless the Hearing Officer determines that another location would be more appropriate. Normally the location for the hearing will be selected for the convenience of all participants. In the event the individual fails to appear at the time and place specified, the record in the case shall be closed and returned to the Manager, who will then make a final determination regarding the eligibility of the individual for DOE access authorization.

(f) At least 7 calendar days prior to the date scheduled for the hearing, the Hearing Officer will convene a prehearing conference for the purpose of discussing stipulations and exhibits, identifying witnesses, and disposing of other appropriate matters. The conference will usually be conducted by telephone.

(g) Hearings shall commence within 90 calendar days from the date the individual's request for hearing is received by the Office of Hearings and Appeals. Any extension of the hearing date past 90 calendar days from the date the request for hearing is received by the Office of Hearings and Appeals shall be approved by the Director, Office of Hearings and Appeals.

§ 710.26 Conduct of hearings.

(a) In all hearings conducted under this subpart, the individual shall have the right to be represented by a person of his own choosing. The individual is responsible for producing witnesses in his own behalf, including requesting the issuance of subpoenas, if necessary, or presenting other proof before the Hearing Officer to support his defense to the allegations contained in the notification letter. With the exception of procedural or scheduling matters, the Hearing Officer is prohibited from initiating or otherwise engaging in ex parte discussions about the case during the pendency of proceedings under this part.

(b) Unless the Hearing Officer finds good cause for granting a waiver of this paragraph or granting an extension of time, in the event that the individual unduly delays the hearing, such as by failure to meet deadlines set by the Hearing Officer, the record shall be closed, and a final decision shall be made by the Manager on the basis of the record in the case.

(c) Hearings shall be open only to DOE Counsel, duly authorized representatives of the staff of DOE, the individual and his counsel or other representatives, and such other persons as may be authorized by the Hearing Officer. Unless otherwise ordered by the Hearing Officer, witnesses shall testify in the presence of the individual but not in the presence of other witnesses.

(d) DOE Counsel shall assist the Hearing Officer in establishing a complete administrative hearing record in the proceeding and bringing out a full and true disclosure of all facts, both favorable and unfavorable, having a bearing on the issues before the Hearing Officer. The individual shall be afforded the opportunity of presenting evidence, including testimony by the individual in the individual's own behalf. The proponent of a witness shall conduct the direct examination of that witness. All witnesses shall be subject to cross- examination, if possible. Whenever reasonably possible, testimony shall be given in person.

(e) The Hearing Officer may ask the witnesses any questions which the Hearing Officer deems appropriate to assure the fullest possible disclosure of relevant and material facts.

(f) During the course of the hearing, the Hearing Officer shall rule on all questions presented to the Hearing Officer for the Hearing Officer's determination.

(g) In the event it appears during the course of the hearing that Restricted Data or national security information may be disclosed, it shall be the duty of the Hearing Officer to assure that disclosure is not made to persons who are not authorized to receive it.

(h) Formal rules of evidence shall not apply, but the Federal Rules of Evidence may be used as a guide for procedures and principles designed to assure production of the most probative evidence available. The Hearing Officer shall admit into evidence any matters, either oral or written, which are material, relevant, and competent in determining issues involved, including the testimony of responsible persons concerning the integrity of the individual. In making such determinations, the utmost latitude shall be permitted with respect to relevancy, materiality, and competency. The Hearing Officer may also exclude evidence which is incompetent, immaterial, irrelevant, or unduly repetitious. Every reasonable effort shall be made to obtain the best evidence available. Subject to §§710.26(l), 710.26(m), 710.(n), 710.26(o), hearsay evidence may in the discretion of the Hearing Officer and for good cause shown be admitted without strict adherence to technical rules of admissibility and shall be accorded such weight as the circumstances warrant.

(i) Testimony of the individual and witnesses shall be given under oath or affirmation. Attention of the individual and each witness shall be directed to 18 U.S.C. 1001 and 18 U.S.C. 1621.

(j) The Hearing Officer shall endeavor to obtain all the facts that are reasonably available in order to arrive at findings. If, prior to or during the proceedings, in the opinion of the Hearing Officer, the allegations in the notification letter are not sufficient to cover all matters into which inquiry should be directed, the Hearing Officer shall recommend to the Operations Office Manager concerned that, in order to give more adequate notice to the individual, the notification letter should be amended. Any amendment shall be made with the concurrence of the local Office of Chief Counsel or the Office of General Counsel in Headquarters cases. If, in the opinion of the Hearing Officer, the circumstances of such amendment may involve undue hardships to the individual because of limited time to answer the new allegations in the notification letter, an appropriate adjournment shall be granted upon the request of the individual.

(k) A written or oral statement of a person relating to the characterization in the notification letter of any organization or person other than the individual may be received and considered by the Hearing Officer without affording the individual an opportunity to cross-examine the person making the statement on matters relating to the characterization of such organization or person, provided the individual is given notice that it has been received and may be considered by the Hearing Officer, and is informed of its contents provided such is not prohibited by paragraph (g) of this section.

(l) Any oral or written statement adverse to the individual relating to a controverted issue may be received and considered by the Hearing Officer without affording an opportunity for cross-examination in either of the following circumstances:

(1) The head of the agency supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of the informant's identity would be substantially harmful to the national interest;

(2) The Secretary or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency as to the reliability of the person and the accuracy of the statement concerned, that:

(i) The statement concerned appears to be reliable and material; and

(ii) Failure of the Hearing Officer to receive and consider such statement would, in view of the access sought to Restricted Data, national security information, or special nuclear material, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify

(A) Due to death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the individual, or

(B) Due to some other specified cause determined by the head of the agency to be good and sufficient.

(m) Whenever procedures under paragraph (l) of this section are used:

(1) The individual shall be given a summary or description of the information which shall be as comprehensive and detailed as the national interest permits, and

(2) Appropriate consideration shall be accorded to the fact that the individual did not have an opportunity to cross-examine such person(s).

(n) Records compiled in the regular course of business, or other physical evidence other than investigative reports obtained by DOE, may be received and considered subject to rebuttal without authenticating witnesses provided that such information has been furnished to DOE by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary to safeguard Restricted Data, national security information, or special nuclear material.

(o) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the individual, may be received and considered provided that:

(1) The Secretary or his special designee for that particular purpose has made a preliminary determination that such physical evidence appears to be material;

(2) The Secretary or his special designee for that particular purpose has made a determination that failure to receive and consider such physical evidence would, in view of the access sought to Restricted Data, national security information, or special nuclear material sought, be substantially harmful to the national security; and

(3) To the extent that national security permits, a summary or description of such physical evidence is made available to the individual. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency shall be considered.

(p) The Hearing Officer may request the Local Director of Security to arrange for additional investigation on any points which are material to the deliberations of the Hearing Officer and which the Hearing Officer believes need further investigation or clarification. In this event, the Hearing Officer shall set forth in writing those issues upon which more evidence is requested, identifying where possible persons or sources from which the evidence should be sought. The Local Director of Security shall make every effort through appropriate sources to obtain additional information upon the matters indicated by the Hearing Officer.

(q) A written transcript of the entire proceedings shall be made and, except for portions containing Restricted Data or national security information, a copy of such transcript shall be furnished the individual without cost.

(r) Whenever information is made a part of the record under the exceptions authorized by paragraphs (l) or (o) of this section, the record shall contain certificates evidencing that the determinations required therein have been made.

§ 710.27 Opinion of the Hearing Officer.

(a) The Hearing Officer shall carefully consider the record in view of the standards set forth herein and shall render an initial opinion as to whether the grant or restoration of access authorization to the individual would not endanger the common defense and security and would be clearly consistent with the national interest. In resolving a question concerning the eligibility of an individual for access authorization under these procedures, the Hearing Officer shall consider the factors stated in paragraph 710.7(c) to determine whether the findings will be adverse or favorable.

(b) In reaching the findings, the Hearing Officer shall consider the demeanor of the witnesses who have testified at the hearing, the probability or likelihood of the truth of their testimony, their credibility, and the authenticity and accuracy of documentary evidence, or lack of evidence on any material points in issue. If the individual is, or may be, handicapped by the non-disclosure to the individual of confidential information or by lack of opportunity to cross-examine confidential informants, the Hearing Officer shall take that fact into consideration.

Possible impact of the loss of the individual's access authorization upon the DOE program shall not be considered by the Hearing Officer.

(c) The Hearing Officer shall make specific findings based upon the record as to the validity of each of the allegations contained in the notification letter and the significance which the Hearing Officer attaches to such valid allegations. These findings shall be supported fully by a statement of reasons which constitute the basis for such findings.

(d) The Hearing Officer's opinion shall be predicated upon the Hearing Officer's findings of fact. If, after considering all the factors in light of the criteria set forth in this subpart, the Hearing Officer is of the opinion that it will not endanger the common defense and security and will be clearly consistent with the national interest to grant or continue access authorization to the individual, the Hearing Officer shall render a favorable opinion; otherwise, the Hearing Officer shall render an adverse opinion.

(e) The Office of Hearings and Appeals shall issue the opinion of the Hearing Officer within 30 calendar days of the receipt of the hearing transcript by the Hearing Officer, or the closing of the record, whichever is later, unless an extension is granted by the Director, Office of Hearings and Appeals. Copies of the Hearing Officer's opinion will be provided to the Office of Security Affairs, the Manager, the individual concerned and his counsel or other representatives, DOE Counsel, and any other party identified by the Hearing Officer. At that time, the individual shall also be notified of his right to request further review of his case pursuant to §710.28.

(f) In the event the Hearing Officer's opinion is favorable to the individual, a copy of the administrative record in the case shall also be provided to the Office of Security Affairs. The Director, Office of Security Affairs will determine whether:

(1) To grant or reinstate the individual's access authorization, or

(2) To refer the case to the Director, Office of Hearings and Appeals, for further review.

(g) In the event the Hearing Officer's opinion is adverse to the individual, and the individual does not file a request for further review pursuant to §710.28, a copy of the administrative record shall be provided to the Director, Office of Security Affairs, who shall make a final determination on the basis of the material contained in the administrative record.

§710.28 Action on the Hearing Officer's opinion.

(a) The Office of Security Affairs or the individual involved may file a request for review of the Hearing Officer's opinion issued under §710.27 within 30 calendar days of receipt of the opinion. Any such request shall be filed with the Director, Office of Hearings and Appeals, and served on the other party.

(b) Within 15 calendar days after filing a request for review under this section, the party seeking review shall file a statement identifying the issues on which it wishes the Director, Office of Hearings and Appeals, to focus. A copy of such statement shall be served on the other party, who may file a response within 20 days of receipt of the statement.

(c) The Director, Office of Hearings and Appeals, may initiate an investigation of any statement contained in the request for review and utilize any relevant facts obtained by such investigation in conducting the review of the Hearing Officer's opinion. The Director, Office of Hearings and Appeals, may solicit and accept submissions from either the individual or the Office of Security Affairs, that are relevant to the review. The Director, Office of Hearings and Appeals, may establish appropriate time frames to allow for such responses. In reviewing the Hearing Officer's opinion, the Director, Office of Hearings and Appeals, may consider any other source of information that will advance the evaluation, provided that both parties are afforded an opportunity to respond to all third person submissions. All information obtained under this section shall be made part of the administrative record.

(d) Within 45 days of the closing of the record, the Director, Office of Hearings and Appeals, shall make specific

findings disposing of each substantial issue identified in a written statement in support of the request for review and the written response submitted by either the individual or the Office of Security Affairs, and shall predicate his opinion on the administrative record, including any new evidence that may have been submitted pursuant to §710.29. If, after considering all the factors in light of the criteria set forth in this subpart, the Director, Office of Hearings and Appeals, is of the opinion that it will not endanger the common defense and security and will be clearly consistent with the national interest to grant or continue access authorization to the individual, the Director, Office of Hearings and Appeals, shall render an opinion favorable to the individual; otherwise, the Director, Office of Hearings and Appeals, shall render an opinion adverse to the individual. The written opinion of the Director, Office of Hearings and Appeals, shall be provided to the Director, Office of Security Affairs, accompanied by the administrative record in the case. The Director, Office of Hearings and Appeals, shall notify the individual of the foregoing action.

(e) Within 30 calendar days of receipt of the opinion of the Director, Office of Hearings and Appeals, the Director, Office of Security Affairs, will make the final determination, based on a complete review of the record, whether access authorization shall be granted or denied, or reinstated or revoked. If, after considering all of the factors in light of the criteria set forth in this subpart, the Director, Office of Security Affairs, determines that it will not endanger the common defense and security and will be clearly consistent with the national interest, access authorization shall be granted to or reinstated for the individual; otherwise, the Director, Office of Security Affairs, shall determine that access authorization shall be denied to or revoked for the individual.

(f) The Director, Office of Security Affairs, shall, through the Director, Office of Safeguards and Security, inform the individual involved and his counsel or representative in writing of the final determination and provide a copy of the written opinion rendered by the Director, Office of Hearings and Appeals. Copies of the correspondence shall also be provided to the Director, Office of Hearings and Appeals, the Manager, DOE Counsel, and any other party. In the event of an adverse determination, the correspondence shall indicate the findings by the Director, Office of Security Affairs, with respect to each allegation contained in the notification letter.

§710.29 New evidence.

(a) In the event of the discovery of new evidence relevant to the allegations contained in the notification letter prior to final determination of the individual's eligibility for access authorization, such evidence shall be submitted by the offering party to the Director, Office of Safeguards and Security. DOE Counsel shall notify the individual of any new evidence submitted by DOE.

(b) The Director, Office of Safeguards and Security, shall:

(1) Refer the matter to the Hearing Officer appointed in the individual's case if the Hearing Officer has not yet issued an opinion. The Hearing Officer getting the application for the presentation of new evidence shall determine the appropriate form in which any new evidence, and the other party's response, shall be received, e.g., by testimony before the Hearing Officer, by deposition or by affidavit.

(2) In those cases where the Hearing Officer's opinion has been issued, the application for presentation of new evidence shall be referred to the Director, Office of Hearings and Appeals, or the Director, Office of Security Affairs, depending upon where the case resides. In the event that the Director, Office of Hearings and Appeals, or Director, Office of Security Affairs, determines that the new evidence should be received, he shall determine the form in which it, and the other party's response, shall be received.

(c) When new evidence submitted by either party is received into the record, the opposing party shall be afforded the opportunity to cross-examine the source of the new information or to submit a written response, unless the information is subject to the exceptions in §710.26 (l) or (o).

§ 710.30 Action by the Secretary.

(a) Whenever an individual has not been afforded an opportunity to cross-examine witnesses who have furnished information adverse to the individual under the provisions of § 710.26 (l) or (o), only the Secretary may issue a final determination denying or revoking the access authorization after personally reviewing the record.

(b) When the Secretary makes a final determination regarding the individual's eligibility for DOE access authorization, the individual will be notified, by the Director, Office of Security Affairs, of that decision and of the Secretary's findings with respect to each allegation contained in the notification letter and each substantial issue identified in the statement in support of the request for review.

(c) Nothing contained in these procedures shall be deemed to limit or affect the responsibility and powers of the Secretary to issue subpoenas or to deny or revoke access to Restricted Data, national security information, or special nuclear material if the security of the nation so requires. The Secretary's authority may not be delegated and may be exercised only when the Secretary determines that the procedures prescribed in § 710.26 (l) or (o) cannot be invoked consistent with the national security, and such determination shall be conclusive.

§ 710.31 Reconsideration of access eligibility.

(a) Where, pursuant to the procedures set forth in §§ 710.20 through 710.30, the Director, Office of Security Affairs, or the Secretary has made a determination granting or reinstating access authorization to an individual, the individual's eligibility for access authorization shall be reconsidered as a new administrative review under the procedures set forth in this subpart when previously unconsidered substantially derogatory information is identified, or the individual violates a commitment or promise upon which the DOE previously relied to favorably resolve an issue of access eligibility.

(b) Where, pursuant to those procedures, the Manager, Director, Office of Security Affairs, or the Secretary has made a determination denying or revoking access authorization to an individual, the individual's eligibility for access authorization may be reconsidered when there is a bona fide offer of employment requiring access to Restricted Data, national security information or special nuclear material, and there is either:

(1) Material and relevant new evidence which the individual and the individual's representatives are without fault in failing to present earlier, or

(2) Convincing evidence of reformation or rehabilitation.

(c) A request for reconsideration shall be submitted in writing to the Manager having jurisdiction over the position for which access authorization is required. A request for reconsideration shall be accompanied by an affidavit setting forth in detail the new evidence or evidence of reformation or rehabilitation. The Manager shall notify the individual as to whether the individual's eligibility for access authorization will be reconsidered and, if so, the method by which such reconsideration will be accomplished.

(d) Final determinations regarding eligibility for DOE access authorization in reconsideration cases shall be made by the Director, Office of Security Affairs.

MISCELLANEOUS

§ 710.32 Terminations.

In the event the individual is no longer an applicant for access authorization or no longer requires access authorization, the procedures of this subpart shall be terminated without a final determination as to the individual's eligibility for access authorization.

§ 710.33 Attorney representation.

In the event the individual is represented by an attorney or other representatives, the individual shall file with the Hearing Officer and DOE Counsel a document designating such attorney or representatives and authorizing one such attorney or representative to receive all correspondence, transcripts, and other documents pertaining to the proceeding under this subpart.

§710.34 Time frames.

Statements of time established for processing aspects of a case under this subpart are the agency's desired time frames in implementing the procedures set forth in this subpart. They shall have no impact upon the final disposition of an access authorization by an Operations Office Manager, the Director, Office of Security Affairs, or the Secretary, and shall confer no rights upon an individual whose eligibility for access authorization is being considered.

Appendix H

United States District Court, Protective Order

APPENDIX H

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No.
	)	
	)	

PROTECTIVE ORDER

This matter comes before the Court upon the Government's Motion for Protective Order to prevent the unauthorized disclosure or dissemination of classified national security information and documents, which will be reviewed or made available to the defendant and his counsel in this case.

Pursuant to Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III (1988) ("CIPA"); Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (the "Security Procedures"); rules 16(d) and 57 of the Federal Rules of Criminal Procedure; the general supervisory authority of the Court; and in order to protect the national security,

IT IS ORDERED:

1. The procedures set forth in this Protective Order, CIPA, and the Security Procedures shall apply to all pretrial, trial, post-trial and appellate matters concerning classified information in this case.

2. As used herein, the terms "classified national security information and documents," "classified information" and "classified documents" refer to :

(1) any classified document (or information contained therein);

(2) verbal classified information known to the defendant or defense counsel;

(3) classified documents and information which have otherwise been made known to the defendant or defense counsel, and which documents have been marked: "Confidential," "Secret" or "Top Secret," or "Sensitive Compartmented Information" where the defendant or defense counsel have been advised in writing from the government of their classified nature.

3. All such classified documents and information contained therein shall remain classified unless the documents bear a clear indication that they have been declassified by the agency or department that is the originating agency of the document or the information contained therein (hereinafter, the "originating agency").

4. The words "documents" or "information" as used in this Order include, but are not limited to, all written or printed matter of any kind, formal or informal, including originals, conforming copies and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), and further include, but are not limited to,

(1) papers; correspondence; memoranda; notes; letters; telegrams; reports; summaries; inter-office and intra-office communications; notations of any sort concerning conversations, meetings or other communications; bulletins; teletypes; telefascimiles; invoices; worksheets; and drafts, alterations, modifications, changes and amendments of any kind to the foregoing.

(2) graphics or oral records or representations of any kind, including, but not limited to, photographs; charts; graphs; microfiche; microfilm; videotapes; sound recordings of any kind; and motion pictures;

(3) electronic, mechanical ro electric records of any kind, including, but not limited to, tapes; cassettes; disks; recordings; films; typewriter ribbons and word-processing disks or tapes; and

(4) information acquired orally.

5. This case involves classified national security information and documents. The storage, handling and control of such documents and information require special security precautions mandated by statute, executive order, and regulation, and access to which requires a special security clearance.

6. The Court has been advised that the government attorneys working on this case, ----- -----, ----- -------, and -------- --------, have the requisite security clearances to have access to the classified documents and information that relate to this case.

7. In accordance with the provisions of CIPA and the Security Procedures, the Court designates --------- --- ------- as Court Security Officer for this case, and --------- ----------, --------- ----------, ---------- ---------- , and ---------- ---------- as alternate Court Security Officers, for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information or documents to be made available to the defendant or his counsel in connection with this case. Defense counsel shall seek guidance from the Court Security Officer with regard to appropriate storage and use of classified

information.

8. This Order shall apply to the defendant, defense counsel and any other person who may require or receive access to classified national security information or documents connected with this case.

9. Defendant and the following attorneys for the defense and their approved employees shall be given access to classified national security documents and information as required by the Government's discovery obligations and as necessary to prepare for proceedings in this case, in accordance with the terms of this Protective Order and upon receipt of the appropriate security clearances: ------. --------, ----- -. ------, ------- -.----------, ----- ------- and ------ -------.

10. Before any person, including the defendant and his counsel, but not including government counsel, appropriately cleared Court personnel, appropriately cleared Department of Justice employees, and appropriately cleared personnel of the originating agencies, shall inspect or review classified national security information involved in this case, he or she must also sign and swear to the Memorandum of Understanding ("MOU") appended to this Protective Order. Each such person executing the MOU must file an executed original with the Court and in addition must provide an executed original to the Court Security Officer.

11. Unless already holding an appropriate security clearance, and approved for access to classified material in the instant case, for the purpose of establishing security clearances necessary for access to classified information that may be involved in this case, Standard

Form 86 ("Security Investigation Data for Sensitive Position"), attached releases, and full fingerprints shall be completed and submitted to the Court Security Officer forthwith by defense counsel, all persons whose assistance the defense reasonably requires, and by such Court personnel as the Court requires for its assistance. The Court Security Officer shall take all reasonable steps to process all security clearance applications.

12. Any request for disclosure of classified information to additional persons not named in paragraph 9 will require the approval of the Court and will be made by motion. The government will be given an opportunity to be heard in response of any defense request for disclosure to a person not named in paragraph 9 above. Any person approved by the Court for disclosure under this paragraph shall be required to receive the appropriate security clearance from the Court Security Officer, to sign and submit to the Court the MOU appended to this Order, and to comply with all terms and conditions of this Order. Any request for security clearances and for access to classified documents and information in this case shall be made to the Court Security Officer, who shall promptly file them.

13. Defense counsel shall be given access between 8 a.m. and 6 p.m., and at all other times including weekends and holidays upon 24 hour notice, to a secure room approved by the Court Security Officer for the storage of classified national security documents and for the preparation of documents which contain classified information. The defendant shall have access to the room only with the presence of defense counsel, and only during the hours of 8 a.m. to 6 p.m. weekdays, unless these hours are amended by Order of Court. No documents containing classified information may be removed from this room unless

authorized by the Court Security Officer.

14. No person who is permitted to inspect and review classified national security information and documents under the terms of this Protective Order shall copy or reproduce any part of them, in any manner or form, except as provided by the Court Security Officer.

15. Classified national security documents and information, and information believed to be classified, shall only be discussed in an area approved by the Court Security Officer, and in which persons not authorized to possess such information cannot overhear such discussions.

16. No one shall discuss classified information related to this case over any standard commercial telephone instruments or office intercommunication systems, or in the presence of any person who has not been granted access to classified information in this case by the Court.

17. Written materials containing classified information prepared for this case by the defendant or defense counsel shall be transcribed, recorded, typed, duplicated, copied or otherwise prepared only by persons who have received access to classified information pursuant to this Order. The Court Security Officer shall not reveal to the government the content of any conversations she/he may hear between defense counsel, their employees, and the defendant, or any of them, nor reveal the nature of the documents being reviewed by them, or the work generated by them.

18. All machines of any kind used in the preparation or transmission of classified information in this case may be used only with the approval of the Court Security Officer and

in accordance with any reasonable instructions the Court Security Officer may issue.

19. Until further order of this Court, all written pleadings of the defendant in this case shall be submitted to the Court Security Officer. The time of physical submission to the Court Security Officer shall be considered the time of filing. The Court Security Officer shall promptly review such pleadings and determine, with the assistance and consultation representatives of the originating agencies, whether any of the material submitted is classified and the level of classification of such material. If the pleading does not contain any classified information, the Court Security Officer shall forward it immediately to the Clerk of the Court for routine filing. If the pleading does contain classified information, or information which might lead to or cause the disclosure of classified information, the Court Security Officer, after consultation with the attorney for the government, defense counsel and the originating agencies, shall: (1) mark it appropriately; (2) provide a marked copy to government and defense counsel; and (3) have it filed under seal and stored under the appropriate security conditions.

20. All written pleadings of the United States which involve classified information shall be forwarded to the Court Security Officer for filing under seal with the Clerk of the Court.

21. Without prior authorization of the Department of Justice or the Court, there shall be no disclosure to any person not named in this Protective Order by defense counsel, defendant or any other person who may later receive the security clearance from the Department of Justice in connection with this case (except to the Court, the Court Security

Officer or government counsel acting in the course of their official duties), of any classified national security information or documents (or information contained therein) until such time, if ever, that such documents or information are openly admitted into evidence during proceedings in this case or otherwise declassified.

22. Those named herein are advised that direct or indirect unauthorized disclosure, retention, or negligent handling of classified documents or information could cause damage, and in some cases, exceptionally grave damage to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. This Protective Order is to ensure that those named herein will never divulge the classified information disclosed to them to anyone who is not now authorized to receive it, without prior written authorization from the originating agency and in conformity with this Order.

23. Persons subject to this Order are advised that any breach of this Order may result in the terminating of their access to classified information and documents and may subject them to contempt of Court. In addition, they are advised that any unauthorized disclosure of classified information may constitute violation of federal criminal laws.

24. All persons given access to classified information pursuant to this Order are advised that such information is now and will forever remain the property of the United States government. Such persons shall return all classified documents which come into their possession, or for which they are responsible because of access pursuant to this Order, upon demand of the Court Security Officer.

25. A copy of this Order shall issue forthwith to defense counsel named herein and

said counsel are required to advise the defendant of the contents of this Order, and to furnish defendant with a copy. The defendant, through counsel, shall forthwith sign the attached MOU and counsel shall forthwith file an executed original with the Court. Furthermore, defense counsel are to provide executed originals of this statement to the Court Security Officer. The signing and filing of this statement by defendant is a condition precedent to the disclosure of classified information to the defendant.

26. Nothing contained in the Memorandum of Understanding signed by defendant, or defendant's consent to the entry of this order, shall be construed as a waiver of any right of the defendant, including any claim raised by the defendant that the provisions of CIPA are unconstitutional.

27. This Order may be amended by the Court upon the showing of good cause.

ORDERED this 4th day of February, 1997 at Alexandria, Virginia.

_____
United States District Judge

WE ASK FOR THIS:
UNITED STATES ATTORNEY

_____
Assistant United States Attorneys

SEEN AND AGREED TO:

_____
Counsel for Defendant

Appendix I

Special Security Agreement

APPENDIX I

SPECIAL SECURITY AGREEMENT

This agreement ("the Agreement") is made this _____ day of _____, 200_ (effective date), by and between [Ultimate Parent], a [country] corporation; [Intermediate Parent], a [State or Country] Corporation (the "Parent Corporation"); [Cleared Corporation], a [State] Corporation (the "Corporation") and the United States Department of Defense (DoD), all of the above collectively "the Parties".

RECITALS

WHEREAS, the Corporation is duly organized and existing under the laws of the State of _____, and has an authorized capital of _____ shares, all of which are common voting shares, par value $_____, and of which, _____ shares are issued and outstanding; and

WHEREAS, [Ultimate Corporation] owns all the outstanding voting shares of [Intermediate Parent]; and

WHEREAS, the Parent Corporation owns the issued and outstanding shares of the Corporation; and

WHEREAS, _____, a public corporation traded on the New York Stock Exchange, owns all the shares of the parent; and

WHEREAS, the Corporation's business consists of _____ that occasionally is installed and/or serviced in environments controlled and of interest to various Departments and Agencies[1] of the United States Government, including, without limitation, the DoD, and require the Corporation to have a facility security clearance; and

WHEREAS, the offices of the Corporation and, possibly, its wholly owned subsidiaries, require facility security clearances[2] issued under that National Industrial Security Program ("NISP") to conduct its business of _____, and the NISP requires that a corporation maintaining a facility security clearance be effectively insulated from foreign ownership, control

---

[1] The Office of the Secretary of Defense (including all boards, councils, staffs, and commands),DoD agencies, and the Departments of Army, Navy, and Air Force (including all of their activities); the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor, and Justice; National Aeronautics and Space Administration; General Services Administration; Small Business Administration; National Science Foundation, Environmental Protection Agency United States Arms Control and Disarmament Agency; Federal Emergency Management Agency; Federal Reserve System; United States Information Agency; International Trade Commission; United States Trade Representative; and the General Accounting Office (the "User Agencies").

[2] An administrative determination that a facility is eligible for access to classified information of a certain category.

or influence ("FOCI"); and

WHEREAS, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I) has determined that the provisions of this Agreement are necessary to enable the United States to protect itself against the unauthorized disclosure of information relating to the national security; and

WHEREAS, the DoD has agreed to grant or continue the facility security clearance(s) of the Corporation and its wholly owned subsidiaries from and after the effective date of this Agreement in consideration of, inter alia, the Parties' execution and compliance with the provisions of the Agreement, the purpose of which is to reasonably and effectively deny the Parent Corporation and all entries which the Parent Corporation either controls, or is controlled by, hereinafter sometimes referred to collectively as the "Affiliates," from unauthorized access to classified[3] and controlled unclassified information[4] and influence over the Corporation's business or management in a manner which could result in the compromise of classified information or could directly and adversely affect the performance of classified contracts; and

WHEREAS, the Corporation has agreed to establish a formal organizational structure procedures: to ensure that protection of classified information entrusted to it and to place the responsibility therefor with a committee of its Board of Directors to be known as the Government Security Committee, all as hereinafter provided; and

WHEREAS, the Parties agree that control of the Corporation should be vested in the Board of Directors of the Corporation; and

WHEREAS, a company under FOCI is not normally authorized to have access to the following classified information.

a. TOP SECRET information;

b. RESTRICTED DATA as defined in the United States Atomic Energy Act of 1954, as amended;

c. Communications Security ("COMSEC") information, except classified keys used to operate secure telephone units (STU III's).

d. Special Access Program information, and

---

[3] Any information that has been determined pursuant to Executive Order 12356 or any predecessor or successor order to require protection against unauthorized disclosure and is so designated. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information.

[4] Unclassified information the export of which is controlled by the International Traffic in Arms Regulations ("ITAR") and/or the Export Administration Regulations ("EAR"). The export of technical data which is inherently military in nature is controlled by the ITAR. The export of technical data which has both military and commercial uses is controlled by the EAR.

e. Sensitive Compartmented Information; and,

WHEREAS, in order to comply fully with the policies of DoD that require a corporation maintaining a facility security clearance to be insulated effectively from undue FOCI, all parties hereto have agreed that management control of the defense and technology security affairs and classified contracts of the Corporation should be vested in resident citizens of the United States who have DoD personnel security clearances[5]; and

WHEREAS, the Parent Corporation and other _____ signatories hereto, by their authorized representatives, hereby affirm that: (a) they will not seek access to or accept U.S. Government classified information or controlled unclassified information entrusted to the Corporation, except as permissible under the NISP and applicable United State Government laws and regulations; (b) they will not attempt to control or adversely influence the Corporation's performance of classified contracts and participation in classified programs; and (c) except as expressly authorized by the Agreement, their involvement (individually and collectively) in the business affairs of the Corporation shall be limited to participation in the deliberation and decisions of the Corporation's Board of Directors and authorized committees thereof; and

WHEREAS, in order to meet DoD's national security objectives in the matter of the Corporation's facility security clearance (s) and to further the Corporation's business objectives, the Parties intend to be bound by the provisions of the Agreement;

NOW THEREFORE, it is expressly agreed by and between the Parties that this Agreement is hereby created and established, subject to the following terms and conditions, to which all of the Parties expressly assent and agree:

ORGANIZATION

ARTICLE I - Management of the Corporation's Business

1.01. Composition of the Corporation Board of Directors.

The Board of Directors of the Corporation ("the Corporation Board"), shall be appointed by the Parent Corporation and shall be composed of: (i) a minimum of _____( ) individuals who have no prior relationship with the Corporation or the Affiliates (the "Outside Directors"), except as otherwise allowed by DoD; (ii) at least one representative of the Parent Corporation (the "Inside Director"); and (iii) one or more cleared officer(s) of the Corporation (the Officer/Director"). The number of Inside Directors shall not exceed the combined total of Outside Directors and Officer/Directors. Except as specifically provided herein, each member of the Corporation Board, however characterized by this Section 1.01, shall have all of the rights, powers, and responsibilities conferred or imposed upon directors of the company, by applicable statutes and regulations, and by the Corporation's charter and by-laws. The Chairman of the Corporation

---

[5] An Administrative determination that an individual is eligible for access to classified information of a certain category.

Board, as well as its principle officers[6], must be resident citizens of the United States who have or who are eligible to possess DoD personnel security clearances at the level of the Corporation's facility security clearances. In addition, the Chairman of the Corporation Board shall not be an Inside Director. All directors of the Corporation shall satisfy the pertinent requirements established in Section 3.01 below. The Outside Directors may not be removed without prior notice to, and approval by, the Defense Security Service ("DSS"). Appointments of new or replacement directors, other than Inside Directors, shall not become final until approved by DSS.

1.02. Actions by the Corporation Board.

a. No action may be taken by the Corporation Board, or any committee thereof, in the absence of a quorum, as defined below.

b. A majority of the Corporation Board, including at least on Inside Director and one Outside Director, shall be necessary to constitute a quorum. With respect to the Government Security Committee (see Section 7.01 below), a majority of the Committee shall be necessary to constitute a quorum. With respect to all other standing committees of the Corporation Board, including the Compensation Committee (see Article VIII below), a majority of such committee, including at least on Outside Director and one Inside Director, shall be necessary to constitute a quorum.

ARTICLE II - Limitations on the Corporation Board

2.01 The Corporation Board shall not be authorized to take any of the actions specified in subsections 2.01a. through 2.01d. below, unless it shall have received, with respect to each such action, the prior written approval of the Parent Corporation:

a. The sale, lease or other disposition of any of the property, assets or business of the Corporation, or the purchase of any property or assets by the Corporation that is other than in the ordinary course of business.

b. The merger, consolidation, reorganization, dissolution or liquidation of the Corporation;

c. The filing or making of any petition under the Federal Bankruptcy Code or any applicable bankruptcy law or other acts of similar character;

d. The initiation of action to terminate this Agreement, except as provided in

---

[6] For purposes of this Agreement, "principle officers" shall have the meaning ascribed to it under the DoD Industrial Security Manual, Appendix D, page 9, viz.: those persons occupying positions normally identified as president, senior vice president, secretary, treasurer and those persons occupying similar positions. In unusual cases, the determination of principal officer status may require a careful analysis of an individual's assigned duties, responsibilities, and authority as officially recorded by the organization. Excluded from this definition are: (i) assistant vice presidents who have no management responsibilities related to performance on classified contracts, (ii) assistant secretaries, and (iii) assistant treasurers.

Section 16.01 below.

ARTICLE III - Qualification, Appointment, and Removal of Directors; Board Vacancies

3.01 During the period that the Agreement is in force, the Corporation Board shall be composed as provided in Section 1.01 hereof, and its members shall meet the following additional requirements:

a. Officers/Directors and Outside Directors shall be resident citizens of the United States and have or be eligible to have DoD personnel security clearances at the level of the Corporation's facility security clearance;

b. Outside Directors shall have been approved by DSS as satisfying the appropriate DoD personnel security requirements and the applicable provisions of the Agreement;

c. The Inside Directors, in their capacity as Directors of the Corporation, shall not have DoD personnel security clearances, regardless of citizenship, and they shall be formally excluded from access to classified information by resolution of the Corporation Board.

3.02. The Parent Corporation, as the sole stockholder of the Corporation, may remove any member of the Corporation Board for any reason permitted by the provisions of applicable state law or the Corporation's Certificate of Incorporation or By-Laws, provided that:

a. The removal of an Outside Director shall not become effective until that director, the Corporation, and DSS have been notified, DSS has approved the removal, and a successor who is qualified to become an Outside Director within the terms of the Agreement has been approved by DSS;

b. Notification to DSS of the removal of a Director shall be the responsibility of the Parent Corporation through the Facility Security Officer of the Corporation, and, except as noted in subsection 3.02c below, must be given at least twenty days prior to the proposed removal date;

c. Notwithstanding the foregoing, however, if immediate removal of any Director is deemed necessary to prevent actual or possible violation of any statue or regulation or actual or possible damage to the Corporation, the Director may be removed at once, although DSS shall be notified prior to or concurrently with such removal.

3.03 In the event of any vacancy on the Corporation Board, however occurring, the Corporation shall give prompt notice of such vacancy to the Parent Corporation and DSS, through its Facility Security Officer, and such vacancy shall be filled promptly by the Parent Corporation. Such a vacancy shall not exist for a period of more than 90 days after the Director's resignation, death, disability or removal unless DSS is notified of the delay.

3.04 Except as provided by this paragraph, the obligation of a Director to abide by and enforce this Agreement shall terminate when the Director leaves office, but nothing herein shall relieve the departing Director of any responsibility that the Director may have, pursuant to the laws

and regulations of the United States, not to disclose classified information or controlled unclassified information obtained during the course of the Director's service on the Corporation Board, and such responsibility shall not terminate by virtue of the Director leaving office. The Corporation's Facility Security Officer shall advise the departing Director of such responsibility when the Director leaves office, but the failure of the Corporation to so advise the Director shall not relieve the Director of such responsibility.

ARTICLE IV - Indemnification and Compensation of Outside Directors.

4.01. The Outside Directors in their capacity as directors of the Corporation shall vote and act on all matters in accordance with their best efforts.[7]

4.02. The Corporation and the Parent Corporation jointly and severally shall indemnify and hold harmless each Outside Director from any and all claims arising from, or in any way connected to, his performance as a director of the Corporation under the Agreement except for his own individual gross negligence or willful misconduct. The Corporation and the Parent Corporation shall advance fees and costs incurred in connection with the defense of such claim. The Parent Corporation or the Corporation may purchase insurance to cover this indemnification.

ARTICLE V - Restrictions Binding on Subsidiaries of the Corporation.

5.01. The parties hereto agree that the provisions of this Agreement restricting unauthorized access to classified information and controlled unclassified information entrusted to the Corporation by entities under FOCI, and all provisions of the Visitation Policy established in Article XI, below shall apply to and shall be made to be binding upon all present and future subsidiaries[8] of all companies controlled by the Corporation that have facility security clearances, or that may be processed for facility security clearance. The Corporation hereby agrees to undertake any and all measures, and provide such authorizations, as may be necessary to effectuate this requirement. The sale of, or termination of the Corporation's control over, any such subsidiary or controlled company shall terminate the applicability to it of the provisions of this Agreement.

5.02. If the Corporation proposes to form a new subsidiary, or to acquire ownership or control of another company, it shall give notice of such proposed action to DSS and shall advise DSS immediately upon consummation of such formation or acquisition,

5.03. It shall be a condition of each such formation or acquisition that all provisions of the

---

[7] For the purposes of the Agreement, the term "best efforts," signifies performance of duties reasonably and in good faith, in the manner believed to be in the best interests of the Corporation but consistent with the national security concerns of the United States, and with such care, including reasonable inquiry, as an ordinarily prudent person in a like position would use under similar circumstances.

[8] The term "subsidiaries" shall, for the purposes of this Agreement, include companies wholly owned by the Corporation or in which the Corporation owns a controlling interest, either directly or through the Corporation's ownership interest in intermediate companies.

Visitation Policy established in Article XI, below and all of the above-described restrictive provisions of the Agreement shall apply to each such company immediately upon consummation of such formation or acquisition, and that the Corporation and the subsidiary or controlled company shall execute a document agreeing that such company shall be bound thereby, and a copy of the executed document shall be forwarded to DSS.

5.04. A document such as described in subsection 5.03 above, shall also be executed and submitted with respect to each present subsidiary of the Corporation, and with respect to any other company which the Corporation presently controls.

5.05. Compliance with this Article V shall not be interpreted as conferring the benefits of this Agreement on those companies. Those companies shall not be entitled to receive a facility security clearance, nor shall they be entitled to access classified information, to perform classified contracts or to participate in classified programs pursuant to this Agreement, solely by virtue of their legal relationship with the Corporation, and their execution of the documents referred to in subsections 5.03 and 5.04 above.

OPERATION

ARTICLE VI - Operation of the Agreement

6.01. The Corporation shall at all times maintain policies and practices to ensure the safeguarding of classified information and controlled unclassified information entrusted to it in the performance of classified contracts and participation in classified programs for the User Agencies in accordance with the Security Agreement (DD Form 441 or its successor form), this Agreement, appropriate contract provisions regarding security, United States export control laws, and the NISP.

a. The following additional protections shall be established in the by-laws and/or resolutions of the governing boards, as appropriate, of the Corporation and the Parent Corporation, and [Ultimate Parent], acknowledged as provided in subsection 6.01.a.1. and 6.01.a.2. below, and shall control the actions of the parties hereto during the term of this Agreement:

1. Pursuant to a resolution of the Corporation Board, which shall not be repealed or amended without approval of DSS, the Corporation shall exclude the Affiliate and all members of its Board of Directors and all of its officers, employees, agents and other representatives of each of them from access to classified information and controlled unclassified information entrusted to the Corporation. The above exclusion shall not, however, preclude the exchange of classified information or controlled unclassified information between the Corporation and the Parent when such exchange is permissible under the NISP and applicable United States laws and regulations.

2. Pursuant to a resolution of the Parent Corporation's Board of Directors, which shall not be repealed or amended without approval of DSS, the Parent Corporation shall formally acknowledge and approve the Corporation's resolution referred to in subsection 6.01.a.1. above, and shall additionally resolve:

(i) To exclude itself and all affiliates and all members of the Boards of Directors and all officers, employees, agents and other representatives of all the foregoing, from access to classified information and controlled unclassified information entrusted to the Corporation, except as expressly permissible pursuant to subsection 6.01.a.1. above; and:

(ii) To grant the Corporation the independence to safeguard classified information and controlled unclassified information entrusted to it; and

(iii) To refrain from taking any action to control or influence the performance of the Corporation's classified contracts or the Corporation's participation in existing classified programs.

b. [Ultimate Patent] shall formally acknowledge and approve the Corporation resolution referenced in 6.01.a.1 above, and the Parent Corporation resolutions referenced in 6.01.a.2. above.

ARTICLE VII - Government Security Committee.

7.01. There shall be established a permanent committee of the Corporation Board, to be known as the Government Security Committee ("GSC"), consisting of all Outside Directors and Officer/Directors to ensure that the Corporation maintains policies and procedures to safeguard classified information and controlled unclassified information in the possession of the Corporation and to ensure that the Corporation complies with the DoD Security Agreement (DD Form 441 or its successor form), this Agreement, appropriate contract provisions regarding security, United States Government export control laws and the NISP. The provisions of this Article VII shall be set forth in the Corporation's By-Laws.

7.02. The GSC Shall designate one of the Outside Directors to serve as Chairman of the GSC.

7.03. The members of the GSC shall exercise their best efforts to ensure the implementation within the Corporation of all procedures, organizational matters and other aspects pertaining to the security and safeguarding of classified and controlled unclassified information called for in this Agreement, including the exercise of appropriate oversight and monitoring of the Corporation's operations to ensure that the protective measures contained in this Agreement are effectively maintained and implemented throughout its duration.

7.04. The Chairman of the GSC shall designate a member to be Secretary of the GSC. The Secretary's responsibility shall include ensuring that all records, journals and minutes of GSC meetings and other documents sent to or received by the GSC are prepared and retained for inspection by DSS.

7.05. A Facility Security Officer ("FSO") shall be appointed by the Corporation. The FSO shall report to the GSC as its principal advisor concerning the safeguarding of classified information. The FSO's responsibility includes the operational oversight of the Corporation's compliance with the requirements of the NISP. The advice and consent of the Chairman of the GSC will be required to select the FSO.

7.06. The members of the GSC shall exercise their best efforts to ensure that the Corporation develops and implements a Technology Control Plan ("TCP"), which shall be subject to inspection by DSS. The GSC shall have authority to establish the policy for the Corporation's TCP. The TCP shall prescribe measures to prevent unauthorized disclosure or export of controlled unclassified information consistent with applicable United States Laws.

7.07. A Technology Control Officer ("TCO") shall be appointed by the Corporation. The TCO shall report to the GSC as its principal advisor concerning the protection of controlled unclassified information. The TCO's responsibilities shall include the establishment and administration of all intracompany procedures to prevent unauthorized disclosure and export of controlled unclassified information and to ensure that the Corporation otherwise complies with the requirements of United States Government export control laws.

7.08. Discussions of classified and controlled unclassified information by the GSC shall be held in closed sessions and accurate minutes of such meetings shall be kept and shall be made available only to such authorized individuals as are so designated by the GSC.

7.09. Upon taking office, the GSC members, the FSO and the TCO shall be briefed by a DSS representative on their responsibilities under the NISP, United States Government export control laws and this Agreement.

7.10. Each member of the GSC, the FSO and the TCO shall exercise his/her best efforts to ensure that all provisions of this Agreement are carried out, that the Corporation's directors, officers, and employees comply with the provisions hereof, and the DSS is advised of any known violation of, or known attempt to violate any provision hereof, appropriate contract provisions regarding security, United States Government export control laws, and the NISP.

7.11. Each member of the GSC shall execute for delivery to DSS, upon accepting his/her appointment, and thereafter, at each annual meeting of GSC with DSS, as established by this Agreement, a certificate acknowledging the protective security measures taken by the Corporation to implement this Agreement. Each member of the GSC shall further acknowledge his/her agreement to be bound by, and to accept his/her responsibilities hereunder and acknowledge that the United States Government has placed its reliance on him/her as a United States citizen and as the holder of a personnel security clearance to exercise his/her best efforts to ensure compliance with the terms of this Agreement and the NISP.

7.12. Obligations and Certification of Cleared Officers

a. Each officer of the Corporation with a personnel security clearance shall exercise his best efforts to ensure that the terms and conditions of the Agreement are complied with by the parties hereto.

b. Upon the effective date of the Agreement and annually thereafter, each such officer shall execute, for delivery to DSS, a certificate: (1) acknowledging the protective security measures taken by the Corporation to implement the Agreement; and (2) acknowledging that the United States Government has placed its reliance on him/her as resident citizen of the United States, and as a holder of a personnel security clearance, to exercise his/her best efforts to ensure compliance with the terms and conditions of the Agreement by the parties hereto.

7.13. Obligations and Certification of Inside Directors

a. Inside Director(s) shall:

1. not have access to classified information and controlled unclassified information entrusted to the Corporation except as permissible under the NISP and applicable United States Government laws and regulations;

2. refrain from taking any action to control or influence the Corporation's classified contracts, its participation in classified programs, or its corporate policies concerning the security of classified information and controlled unclassified information;

3. neither seek nor accept classified information or controlled unclassified information entrusted to the Corporation, except as permissible under the NISP and applicable United States Government laws and regulations; and

4. advise the GSC promptly upon becoming aware of: (i) any violation or attempted violation of this Agreement or contract provisions regarding industrial security, export control; or (ii) actions inconsistent with the NISP or applicable United States Government laws or regulations.

b. Upon accepting appointment, each Inside Director shall execute for delivery to DSS a certificate affirming such Director's agreement to be bound by, and acceptance of the responsibilities imposed by the Agreement, and further acknowledging and affirming the obligations set forth in 7.13.a. above.

ARTICLE VIII - Compensation Committee

8.01. The Corporation Board shall establish a permanent committee of the Board, consisting of at least one Outside Director and one Inside Director, to be known as the Compensation Committee. The Compensation Committee shall be responsible for reviewing and approving the Corporation Board's recommendation for the annual compensation of the Corporation's principal officers, as defined herein.

ARTICLE IX - Annual Review and Certification

9.01. Representative of DSS, the Corporation's Board, the Corporation's Chief Executive Officer, the Corporation's Chief Financial Officer, the FSO, and the TCO shall meet annually to review the purpose and effectiveness of this Agreement and to establish a common understanding of the operating requirements and how they will be implemented. These meetings shall include a discussion of the following:

a. Whether this Agreement is working in a satisfactory manner;

b. Compliance or acts of noncompliance with this Agreement, NISP rules, or other applicable laws and regulations;

c. Necessary guidance or assistance regarding problems or impediments associated with the practical application or utility of the Agreement; and

d. Whether security controls, practices or procedures warrant adjustment.

9.02. The Chief Executive Officer of the Corporation and the Chairman of the GSC shall submit to DSS one year from the effective date of the Agreement and annually thereafter an implementation and compliance report which shall be executed by all members of the GSC. Such reports shall include that following information:

a. A detailed description of the manner in which the Corporation is carrying out its obligation under the Agreement;

b. A detailed description of changes to security procedures, implemented or proposed, and the reasons for those changes;

c. A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of what steps were taken to prevent such acts from occurring in the future;

d. A description of any changes, or impending changes, to any of the Corporation's top management including reasons for such changes;

e. A statement, as appropriate that a review of the records concerning all visits and communications between representatives of the Corporation and the Affiliates have been accomplished and the records are in order;

f. A detailed chronological summary of all transfers of classified or controlled unclassified information, if any, from the Corporation to the Affiliates, complete with an explanation of the United States Governmental authorization relied upon to effect such transfers. Copies of approved export licenses covering the reporting period shall be appended to the report; and

g. A discussion of any other issues that could have a bearing on the effectiveness or implementation of this Agreement.

ARTICLE X - Duty to Report Violations of the Agreement.

10.01. The Parties to this Agreement, except DoD, agree to report promptly to DSS all instances in which the terms and obligations of this Agreement may have been violated.

CONTACTS AND VISITS

ARTICLE XI - Visitation Policy.

11.01. The Chairman of the GSC shall designate at least two Outside Directors who shall

have authority to review, approve, and disapprove requests for visits[9] to the Corporation by all personnel who represent the Affiliates, including all of the directors, officer, employees, representatives, and agents of each, and proposed visits to any Affiliate by all personnel who represent the Corporation, (including all of its directors, employees, officers, representatives, and agents, except for the Inside Director), as well as visits between or among such personnel at other locations (herein "visit" or "visits"). A record of all visit requests, including the decisions to approve or disapprove, and information regarding consummated visits, such as, date, place, personnel involved and summary of material discussion or communication, shall be maintained by the designated Outside Director and shall be periodically reviewed by the GSC.

11.02. Except for certain Routine Business Visits, as defined in Section 11.05 below, all visits must be approved in advance by the one of the Outside Directors designated by the GSC Chairman to act on such matters. All requests for visits shall be submitted or communicated to the FSO for routing to the designated Outside Director. Although strictly social visits at other locations between the Corporation personnel and personnel representing the Affiliates are not prohibited, written reports of such visits must be submitted after the fact to the FSO for filing with, and review by, the designated Outside Director and the GSC.

11.03. A written request for approval of a visit must be submitted to the FSO no less than seven (7) calendar days prior to the date of the proposed visit. If a written request cannot be accomplished because of an unforeseen exigency, the request may be communicated via telephone to the FSO and immediately confirmed in writing; however, the FSO may refuse to accept any request submitted less than seven (7) calendar days prior to the date of the proposed visit if the FSO determines that there is insufficient time to consider the request. The exact purpose and justification for the visit must be set forth in detail sufficient to enable one of the designated Outside Directors to make an informed decision concerning the proposed visit, and the FSO may refuse to accept any request that the FSO believes lacks sufficient information. Each proposed visit must be individually justified and a separate approval request must be submitted for each.

11.04. The FSO shall advise one of the designated Outside Directors of a request for approval of a visit (other than a Routine Business Visit) as soon practicable after receipt of the written request. The designated Outside Director shall evaluate the request as soon as practicable after receiving it. The Outside Director may approve or disapprove the request, or disapprove the request pending submittal of additional information by the requester. The Outside Director's decision shall be communicated to the requester by any means and it shall be confirmed in writing when practicable, at least one day prior to the date of the proposed visit, but in no event later than six (6) calendar days after its receipt by the FSO. A chronological file of all documentation associated with meetings, visitations, and communications (contact reports), together with records of approvals and disapprovals, shall be maintained by the FSO for inspection by DSS. At the time of each GSC meeting, the Outside Directors of the Corporation shall review such documentation filed since the last meeting to ensure adherence to approved

---

[9] As used in the Agreement, the term "visits" includes meetings at any location within or outside the United States, including but not limited to any facility owned or operated by the Corporation or any Affiliates, whether occurring in person or via electronic means, including but not limited to telephone conversations, teleconferences, video conferences, or electronic mail.

procedures by the requesters and the designated Outside Director and to verify that sufficient and proper justification has been furnished for approved visits.

11.05. Routine Business Visits

a. Routine Business Visits, as defined in 11.05.b below, may be approved by the FSO, in the FSO's discretion, without advance approval by one of the designated Outside Directors. Requests for Routine Business Visits must be submitted in advance and in writing to the FSO, and shall state the basis upon which the requester deems the visit to be a Routine Business Visit. Such requests must include sufficient information to enable the FSO to make an informed decision concerning the proposed visit. The FSO, in the FSO's discretion, may refuse to accept any request that the FSO believes lacks sufficient information and may refer any request to the designated Outside Director for evaluation, notwithstanding its designation as a Routine Business Request. Any request that the FSO believes is not properly characterized as a Routine Business Visit shall be referred to the designated Outside Director who shall evaluate the request in accordance with the terms of the Agreement.

b. Routine Business Visits are in general those that are made in connection with the regular day-to-day business operations of the Corporation, do not involve the transfer or receipt of classified information or controlled unclassified information and pertain only to the commercial aspects of the Corporation's business. Routine Business Visits include:

(i) Visits for the purpose of discussing or reviewing such commercial subjects as the following: company performance versus plans or budgets; inventory, accounts receivable, accounting and financial controls; implementation of business plans; and implementation of technical development programs;

(ii) Visits of the kind made by commercial suppliers in general regarding the solicitation of orders, the quotation of prices, or the provision of products and services on a commercial basis;

(iii) Visits concerning fiscal, financial or legal matters involving compliance with the requirements of any foreign or domestic governmental authority responsible for regulating or administering the public issuing of or transactions involving stocks and securities; and

(iv) Visits concerning marketing and technical activities relating to the import or export of products requiring compliance with regulations of United States departments or agencies, including but not limited to the Departments of Defense, Commerce, State, and Treasury.

11.06. Special Provision Concerning Subsidiaries

Anything to the contrary notwithstanding, the notice and approval of visitation restrictions contemplated in the Agreement shall not apply to visits between the Corporation and its subsidiaries. However, visits between the Corporation's subsidiaries and any Affiliate shall be subject to the visitation approval procedures set forth herein.

11.07. Discretion to Alter Notice or Approval Requirements

Anything foregoing to the contrary notwithstanding, the GSC, in its reasonable business discretion and consistent with its obligation to safeguard classified information and controlled unclassified information in the Corporation's possession may, with the approval of DSS:

a. Designate specific categories of visit requests other than those enumerated above as "Routine Business Visits" not requiring the advance approval of the designated Outside Director; or

b. Determine that, due to extraordinary circumstances involving the security of classified information and/or controlled unclassified information, certain specific types of visits which might have otherwise be considered "Routine Business Visits" under the terms of the Agreement are to be allowed only if the approval of the designated Outside Director is obtained in advance.

11.08. Maintenance of Records for DSS Review

A chronological file of all visit requests, reports of visits, and contact reports, together with appropriate approvals or disapprovals pursuant to the Agreement shall be maintained by the GSC for review by DSS.

REMEDIES

ARTICLE XII - DoD Remedies.

12.01. DoD reserves the right to impose any security safeguard not expressly contained in this Agreement that it believes is necessary to ensure that the subsidiaries and Affiliates are denied unauthorized access to classified and controlled unclassified information.

12.02. Nothing contained herein shall limit or affect the authority of the head of a United States Government agency[10] to deny, limit or revoke the Corporation's access to classified and controlled unclassified information under its jurisdiction if the national security requires such action.

12.03. The Parties hereby assent and agree that the United States Government has the right, obligation and authority to impose any or all of the following remedies in the event of a material breach of any term hereof:

a. The novation of the Corporation's classified contracts to another contractor. The costs of which shall be borne by the Corporation;

b. The termination of any classified contracts being performed by the Corporation and the denial of new classified contracts for the Corporation;

c. The revocation of the Corporation's facility security clearance;

d. The suspension or debarment of the Corporation from participation in all Federal

[10] The term "agency" has the meaning provided at 5 U.S.C. 552(f).

government contracts, in accordance with the provisions of the Federal Acquisition Regulations; and

e. The suspension or restriction of any or all visitation privileges.

12.04. Nothing in the Agreement limits the right of the Unites States Government to pursue criminal sanctions against the Corporation, or any Affiliates, or any director, officer, employee, representative or agency of any of these companies, for violations of the criminal laws of the United States in connection with their performance of any of the obligations imposed by this Agreement, including but not limited to any violations of the False Statements Act, 18 U.S.C. 1001, or the False Claims Act 18 U.S.C. 287.

ADMINISTRATION

ARTICLE XIII - Notices.

13.01. All notices required or permitted to be given to the Parties hereto shall be given by mailing the same in a sealed postpaid envelope, via registered or certified mail, or sending the same by courier or facsimile, addressed to the addresses shown below, or to such other addresses as the Parties may designate from time to time pursuant to this Section:

For the Corporation: _____.

For the Parent Corporation: _____.

For the Ultimate Parent: _____.

For DSS: Defense Security Service
Deputy Director for Policy

ARTICLE XIV - Inconsistencies with Other Documents

14.01. In the event that any resolution, regulation or bylaw of any of the Parties to the Agreement is found to be inconsistent with any provision hereof, the terms of this Agreement shall control.

ARTICLE XV - Governing Law; Construction.

15.01. This Agreement shall be implemented so as to comply with all applicable United States laws and regulations. To the extent consistent with the right of the United States hereunder, the laws of the State of _____ shall apply to questions concerning the rights, powers, and duties of the Corporation and the Parent Corporation under, or by virtue of this Agreement.

15.02. In all instances consistent with the context, nouns and pronouns of any gender shall be construed to include the other gender.

TERMINATION

ARTICLE XVI - Termination, Amendment and Interpretations of this Agreement.

16.01. This Agreement may only be terminated by DSS as follows:

a. In the event of sale of the business or all the shares to a company or person not under FOCI;

b. When DSS determines that existence of this Agreement is no longer necessary to maintain a facility security clearance for the Corporation;

c. When DSS determines that continuation of a facility security clearance for the Corporation is no longer necessary;

d. When DSS determines that there has been a breach of this Agreement that requires it to be terminated or when DSS otherwise determines that termination is in the national interest;

e. When DSS otherwise determines that termination is in the national interest;

f. Five (5) days from the effective date of this Agreement if, at least ninety (90) days before that, the Corporation petitions DSS to terminate this agreement; and

g. When the Parent Corporation and the Corporation for any reason and at anytime, petition DSS to terminate this Agreement. However, DSS has the right to receive full disclosure of the reason or reasons therefor, and has the right to determine, in its sole discretion, whether such petition should be granted.

16.02. Unless it is terminated earlier under the provisions of paragraph 16.01, this agreement shall expire ten (10) years from the date of execution without any action being required of any of the parties to the agreement. However, if the parent Corporation and the Corporation together request that DSS continue the agreement past the expiration date, DSS may extend the term of the agreement while a new agreement is being negotiated. Any request to extend the term of the agreement made under this paragraph shall be submitted to DSS no later than ninety (90) days prior to the expiration date of the agreement.

16.03. If DoD determines that this Agreement should be terminated for any reason, DSS shall provide the Corporation and the Parent Corporation with thirty (30) days written advance notice of its intent and the reasons therefor.

16.04. DoD is expressly prohibited from causing a continuation or discontinuation of this Agreement for any reason other than the national security of the United States.

16.05. This Agreement may be amended by an agreement in writing executed by all the Parties.

16.06. The Parties agree that any questions concerning interpretations of this Agreement, or whether a proposed activity is permitted hereunder, shall be referred to DSS and DoD shall serve as final arbiter/interpreter of such matters.

ARTICLE XVII - Place of Filing

17.01. Until the termination of the Agreement, one original counterpart shall be filed at the office of the Corporation, located in [CITY], [STATE] and such counterpart shall be open to the inspection of the Parent Corporation during normal business hours.

EXECUTION

This Agreement may be executed in several counterparts, each of which shall be deemed to be an original, and all of such counterparts shall together constitute but one and the same instrument.

IN WITNESS WHEREOF, the Parties hereto have duly executed the Agreement which shall not become effective until duly executed by the DoD.

_____,Inc.

_____
Signature of Witness

by: _____
President,_____, Inc.

_____
Signature of Witness

by:_____
Senior Vice President,_____,Inc.

Effective Date: _____

_____
Deputy Director for Policy, Defense Security Service (FOR THE DEPARTMENT OF DEFENSE)

ATTACHMENTS

a. Resolution Establishing Security Procedures and Authorizing Special Security Agreement.

b. Resolution Excluding (insert name of Shareholder) from Access to Classified Information and Authorizing Special Security Agreement.

c. Special Security Agreement Certificate.

d. Government Security Committee Member Certificate

e. (Inside Director) Special Security Agreement Certificate.

UNANIMOUS CONSENT OF THE BOARD OF DIRECTOR OF
(Insert name of Corporation)

RESOLUTION ESTABLISHING SECURITY PROCEDURES AND
AUTHORIZING SPECIAL SECURITY AGREEMENT

We, the undersigned, being all of the members of the Board of Directors of (insert name of Corporation), a corporation duly organized and existing under the laws of the State of _____, DO HEREBY CONSENT TO AND APPROVE THE ADOPTION OF the following recitals and resolutions:

WHEREAS (insert name of Shareholder), a (insert name of State or Country) corporation, owns all voting shares of the outstanding stock of (insert name of Corporation) and (insert name of ultimate Shareholder, if any), a (insert name of Country); company, through (insert names and State or Country of all indirect Shareholders existing between the Shareholder and ultimate Shareholder, if any), indirectly owns all the voting shares of the outstanding stock of (insert name of Shareholder); and

WHEREAS (insert name of ultimate Shareholder), (insert name of Shareholder),* (insert name of Corporation), and the United State Department of Defense ("DoD") entered into a Special Security Agreement ("the Agreement"), dated _____; and

WHEREAS under paragraph 7 of the Agreement (insert name of Corporation) must take certain protective measures so that (insert name of Corporation) shall at all time maintain policies and practices that assure the safeguarding of classified information and the performing of classified contracts or programs for the United States User Agencies in accordance with the Department of Defense Security Agreement (DD Form 441), the Agreement, appropriate contract provisions relating to security, and the National Industrial Security Program Operating Manual NISPOM), DoD 5220 22-M, including, in accordance with paragraph 7.01, revision of By-Laws of (insert name of Corporation) to establish a permanent committee of the (insert name of Corporation) Board of Directors consisting of all the outside directors of (insert name of Corporation) and the (insert name of Corporation) corporate officer/directors to be known as the Government Security Committee.

NOW, THEREFORE, BE IT RESOLVED that:

1. (insert name of Corporation), shall at all times maintain policies and practices that assure the safeguarding of classified information and the performing of classified contracts and programs for the United States User Agencies in accordance with the Department of Defense Security Agreement (DD Form 441), the Agreement, appropriate contract provisions regarding security, and the NISPOM, DoD 5220 22-M.

2. The By-Laws of (insert name of Corporation) are revised to establish a permanent committee of the (insert name of corporation) Board of Directors consisting of all the outside directors of (insert name of Corporation) and the (insert name of the Corporation) corporate officers/directors to be known as Government Security Committee.

*List all firms between the ultimate Shareholder and the Corporation.

3. The Government Security Committee shall assure that (insert name of Corporation) maintains policies and practices to safeguard classified information in the possession of (insert name of Corporation) consistent with the terms of the Department of Defense Security Agreement (DD Form 441) and the Agreement.

4. The Government Security Committee shall be responsible for the implementation of the Agreement within (insert name of Corporation) including the exercise of appropriate oversight ant monitoring of (insert name of Corporation) operations to assure that the protective measures contained in the Agreement are implemented effectively and maintained throughout the duration of the Agreement.

5. The members of the Government Security Committee shall be cleared to the level of the facility security clearance of (insert name of Corporation) and shall be specifically approved for this function by the Defense Security Service ("DSS").

6. One of the outside directors shall be designated as Chairman of the Government Security Committee.

7. At least one of the outside directors shall attend all (insert name of Corporation) Board of Directors meetings and (insert name of Corporation) Board of Directors committee meetings in order for there to be a quorum.

8. One of the (insert name of Corporation) officers on the Government Security Committee shall be designated by the Government Security Committee to assure that all records, journals, and minutes of the Government Security Committee meetings or other communications of the Government Security Committee are maintained and readily available for DSS inspections.

9. Discussions of classified matters by the Government Security Committee shall be held in closed sessions and accurate minutes of such meetings shall be kept and shall be available only to such authorized individuals as are identified by the Government Security Committee.

10. Upon taking office, the Government Security Committee members will be briefed by a DSS representative on their responsibilities under DoD security regulations and the Agreement.

11. Each member of the Government Security Committee, upon accepting such appointment and annually thereafter, shall acknowledge by certificate in the form attached hereto, that the United States Government has placed its reliance on them as United States citizens and as holders of personnel security clearances to exercise all appropriate aspects of the Agreement and to assure that the members of the (insert name of Corporation) Board of Directors, (insert name of Corporation) officer, and (insert name of Corporation) employees comply with the provisions of the Agreement, and that DSS is advised of any violation of, or attempt to violate, any undertaking in Agreement, appropriate contract provisions regarding security or the NISPOM, (DoD 5220 22-M), of which they are aware.

12. A report by the Government Security Committee as to the implementation of and compliance with the Agreement shall be delivered annually to the DSS Cognizant Security Office.

RESOLVED FURTHER that the action of the President of (insert name of Corporation) in

executing and delivering the Agreement be and hereby is ratified and affirmed and that the Agreement be and hereby is adopted and approved in substantially the form attached to this written consent.

RESOLVED FURTHER that the appropriate officer or officers of (insert name of Corporation) be and hereby are authorized to take such other actions as may be necessary to implement the provisions of the Agreement.

This Consent may be signed in several counterparts and all such counterparts taken together shall be taken together as one. The number of counterparts that in the aggregate contain the signature of all members of the Board of Directors shall constitute the binding action of the Board.

DATED: _____

_____	_____
Director	Director
_____	_____
Director	Director
_____	_____
Director	Director
_____	_____
Director	Director

UNANIMOUS CONSENT OF THE BOARD OF DIRECTORS OF
(insert name of Shareholder)**

RESOLUTION EXCLUDING (insert name of Shareholder)
FROM ACCESS TO CLASSIFIED INFORMATION AND AUTHORIZING
SPECIAL SECURITY AGREEMENT

We, the undersigned, being all the members of the Board of Directors of (insert name of Shareholder) a corporation duly organized and existing under the laws of (insert name of State or Country), DO HEREBY CONSENT TO AND APPROVE THE ADOPTION OF the following recitals and resolution:

WHEREAS, (insert name of Shareholder), a (insert name of State or Country) corporation, owns all voting shares of the outstanding stock of (insert name of Corporation), a (insert State) corporation, and (insert name of indirect ultimate Shareholder, if any), a (insert name of State or Country) company, through (insert names and State or Country of all indirect Shareholders existing between the Shareholder and ultimate Shareholder, if any), indirectly owns all the voting shares of the outstanding stock of (insert name of shareholder); and

WHEREAS, (insert name of ultimate Shareholder), (insert name of Shareholder),* (insert name of Corporation), and the United Sates Department of Defense ("DoD") entered into a Special Security Agreement (the "Agreement"), dated _____; and

WHEREAS, one of the requirements of the Agreement for the issuance of an unrestricted facility security clearance to (insert name of Corporation)is the adoption by the Board of Directors of (insert name of Shareholder) of a resolution, which cannot be amended without notification to DoD, that excludes the members of its Board of Directors and its officers, employees representatives, and agents from access to classified information in the possession of (insert name of Corporation).

NOW, THEREFORE, BE IT RESOLED that in accordance with and subject to the terms of the Agreement:

1. (insert name of Shareholder), the members of its Board of Directors employees, representatives, and agents, as such, shall be excluded from access to all classified information in the possession of (insert name of Corporation). This prohibition shall not apply if access to classified information is authorized by the provisions of the NISPOM, if an appropriate United States export license has been granted, and if a favorable foreign disclosure decision has been made by DoD, when required.

2. (insert name of Shareholder), as the sole shareholder of (insert name of Corporation), hereby grants to (insert name of Corporation) the independence to safeguard classified information in (insert name of Corporation)'s possession and agrees that it will not influence adversely (insert name of Corporation) classified contracts or programs.

*List all firms between the ultimate Shareholder and the Corporation.
**This Board Resolution must be completed by all Shareholder firms in the chain of ownership.

RESOLVED FURTHER that paragraph 7.01 of the Agreement as it relates to the Government Security Committee and the resolution of the (insert name of Corporation) Board of Directors, adopted by unanimous written consent and dated _____, as it relates to the Government Security Committee be and said terms of the Agreement and the resolution hereby are incorporated into by reference and made a part of the By-Laws of (insert name of Corporation).

RESOLVED FURTHER that the action of the Chairman of the Board of (insert name of Shareholder) in executing and delivering the Agreement be and hereby is ratified and affirmed, and that the appropriate officer or officers of (insert name of Shareholder) be and hereby are authorized to take such other actions as may be necessary to implement the provisions thereof.

This Consent may be signed in several counterparts and all such counterparts taken together shall be taken together as one. The number of counterparts that in the aggregate contain the signatures of all member of the Board of Directors shall constitute the binding action of the Board.

DATED: _____

_____	_____
Director	Director
_____	_____
Director	Director
_____	_____
Director	Director
_____	_____
Director	Director

SAMPLE

SPECIAL SECURITY AGREEMENT CERTIFICATE

Pursuant to the provisions of the Department of Defense Industrial Security Regulation, 5220.22-R, and the proposed Special Security Agreement among the Department of Defense (list subject corporation and all parent corporations),_____

_____

_____

_____

_____, under which I will be an Outside Director, the following assurances are provided:

1. I am a United States citizen.

2. I currently reside within the continental United States.

3. I presently hold a personnel security clearance at the level _____. (or) I am willing to apply for a personnel security clearance in accordance with the National Industrial Security Program Operating Manual, DoD 5220.22-M.

4. I understand my personnel security clearance must be maintained while serving as an Outside Director for _____.

5. I am a completely disinterested individual with no prior involvement with either (insert name of cleared company) or any of its affiliate or the corporate body in which it is located or the (insert name of foreign interest) or any of its affiliates.

6. I fully understand the functions and the responsibilities of an Outside Director of _____, I am willing to accept those responsibilities.

Signed: _____

Dated: _____

Witness: _____
(NAME TYPED OR PRINTED)

GOVERNMENT SECURITY COMMITTEE MEMBER CERTIFICATE

By execution of this Certificate, I acknowledge the protective security measures that have been taken by _____ through resolutions dated _____, to implement the Special Security Agreement (the "Agreement"), copies of which are attached.

I further acknowledge that the United States Government has placed its reliance on me as a United States citizen and as a holder of a personnel security clearance to exercise all appropriate aspects of the Agreement, to assure that members of the _____ Board of Directors, _____ officers, and _____ employees comply with the provisions of the Agreement; and to assure that the Defense Security Service is advised of any violation of, or attempt to violate any undertaking in the Agreement, appropriate contract provisions regarding security or the National Industrial Security Program Operating Manual, DoD 5220.22-M, of which I am aware.

Dated: _____

Signed: _____

_____
(Name Printed or Typed)

(INSIDE DIRECTOR)
SPECIAL SECURITY AGREEMENT CERTIFICATE

I acknowledge that in my capacity as a representative of _____ parent, _____ have been excluded from access to classified information and export-controlled technical data in the possession of _____ on in accordance with the terms of a resolution by the Board of Directors of _____, dated _____, 200_, and the Special Security Agreement entered into among _____ and the United States Department of Defense, dated _____, 200_.

I certify that:

1. I have waived any right to have access to classified information and export-controlled technical data held by _____ except as permissible under the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22M, and applicable United States laws and regulations;

2. I will not adversely influence _____ classified contracts or programs or corporate policies regarding the security of classified information and export controlled technical data;

3. I will not seek and have not obtained classified information or export controlled technical data in the possession of _____ except as permissible under the NISPOM and applicable United States laws and regulations;

4. If I become aware of any violations of the Special Security Agreement or contract provisions regarding industrial security or actions inconsistent with the NISPOM or applicable United States laws and regulations, I will promptly notify the _____ Government Security Committee established by subsection 7(b) of the Special Security Agreement.

Dated: _____

Signature: _____
(Name Typed or Printed)

Witness: _____

_____
(Name Type or Printed)

nas.03a

Appendix J

Questionnaire for National Security Positions, Standard Form 86

Standard Form 86 (EG)
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206-0007
NSN 7540-00-634-4036
86-111

Part 1

Investigating Agency Use Only | Codes | Case Number

Agency Use Only *(Complete items A through P using instructions provided by the Investigating agency).*

A Type of Investigation	B Extra Coverage	C Sensitivity Level	D Access	E Nature of Action Code	F Date of Action	Month	Day	Year		
G Geographic Location	H Position Code	I Position Title								
J SON	K Location of Official Personnel Folder	☐ None ☐ NPRC ☐ At SON	Other Address						ZIP Code	
L SOI	M Location of Security Folder	☐ None ☐ At SOI ☐ NPI	Other Address						ZIP Code	
N OPAC-ALC Number	O Accounting Data and/or Agency Case Number									
P Requesting Official	Name and Title	Signature	Telephone Number ( )	Date						

Persons completing this form should begin with the questions below.

1 FULL NAME • If you have only initials in your name, use them and state (IO). • If you have no middle name, enter "NMN". • If you are a "Jr.," "Sr.," "II," etc., enter this in the box after your middle name.

2 DATE OF BIRTH

Last Name	First Name	Middle Name	Jr., II, etc.	Month	Day	Year

3 PLACE OF BIRTH - Use the two letter code for the State.

City	County	State	Country *(if not in the United States)*

4 SOCIAL SECURITY

5 OTHER NAMES USED
Give other names you used and the period of time you used them *(for example: your maiden name, name(s) by a former marriage, former name(s), alias(es), or nickname(s))*. If the other name is your **maiden name**, put **"nee"** in front of it.

	Name	Month/Year	Month/Year
#1			To
#2			To
#3			To
#4			To

6 OTHER IDENTIFYING INFORMATION

Height *(feet and inches)*	Weight *(pounds)*	Hair Color	Eye Color	Sex *(Mark one box)*
				☐ Female ☐ Male

7 TELEPHONE NUMBERS

Work *(Include Area Code and extension)*	Home *(Include Area Code)*
☐ Day ☐ Night ( )	☐ Day ☐ Night ( )

8 CITIZENSHIP

a Mark the box at the right that reflects your current citizenship status, and follow its instructions.

- ☐ I am a U.S. citizen or national by birth in the U.S. or U.S. territory/possession. *(Answer items b and d)*
- ☐ I am a U.S. citizen, but I was NOT born in the U.S. *(Answer items b, c and d)*
- ☐ I am not a U.S. citizen. *(Answer items b and e)*

b Your Mother's Maiden Name

c UNITED STATES CITIZENSHIP If you are a U.S. citizen, but were not born in the U.S., provide information about one or more of the following proofs of your citizenship.

Naturalization Certificate *(Where were you naturalized?)*

Court	City	State	Certificate Number	Month/Day/Year Issued

Citizenship Certificate *(Where was the certificate issued?)*

City	State	Certificate Number	Month/Day/Year Issued

State Department Form 240 - Report of Birth Abroad of a Citizen of the United States

Give the date the form was prepared and give an explanation if needed.	Month/Day/Year	Explanation

U.S. Passport

This may be either a current or previous U.S. Passport.	Passport Number	Month/Day/Year Issued

d DUAL CITIZENSHIP If you are (or were) a dual citizen of the United States and another country, provide the name of that country in the space to the right. Country

e ALIEN If you are an alien, provide the following information:

	City	State	Date You Entered U.S. Month	Day	Year	Alien Registration Number	Country(ies) of Citizenship
Place You Entered the United States:							

9 WHERE YOU HAVE LIVED

List the places where you have lived, beginning with the most recent (#1) and working back 7 years. All periods must be accounted for in your list. Be sure to indicate the actual physical location of your residence: do not use a post office box as an address, do not list a permanent address when you were actually living at a school address, etc. Be sure to specify your location as closely as possible: for example, do not list only your base or ship, list your barracks number or home port. You may omit temporary military duty locations under 90 days (list your permanent address instead), and you should use your APO/FPO address if you lived overseas

For any address in the last 5 years, list a person who knew you at that address, and who preferably still lives in that area (do not list people for residences completely outside this 5-year period, and do not list your spouse, former spouses, or other relatives). Also for addresses in the last five years, if the address is "General Delivery," a Rural or Star Route, or may be difficult to locate, provide directions for locating the residence on an attached continuation sheet.

#1 Month/Year To Present	Month/Year	Street Address		Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knows You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )
#2 Month/Year To	Month/Year	Street Address		Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )
#3 Month/Year To	Month/Year	Street Address		Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )
#4 Month/Year To	Month/Year	Street Address		Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )
#5 Month/Year To	Month/Year	Street Address		Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )

10 WHERE YOU WENT TO SCHOOL

List the schools you have attended, beyond Junior High School, **beginning with the most recent (#1) and working back 7 years**. List College or University degrees and the dates they were received. If all of your education occurred more than 7 years ago, list your most recent education beyond high school, no matter when that education occurred.

- Use one of the following codes in the "Code" block:

  1 - High School **2** - College/University/Military College **3** - Vocational/Technical/Trade School

- For schools you attended in the past 3 years, list a person who knew you at school (an instructor, student, etc.). Do not list people for education completely outside this 3-year period.

- For correspondence schools and extension classes, provide the address where the records are maintained.

#1 Month/Year To	Month/Year	Code	Name of School		Degree/Diploma/Other			Month/Year Awarded
Street Address and City (Country) of School							State	ZIP Code
Name of Person Who Knew You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )
#2 Month/Year To	Month/Year	Code	Name of School		Degree/Diploma/Other			Month/Year Awarded
Street Address and City (Country) of School							State	ZIP Code
Name of Person Who Knew You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )
#3 Month/Year To	Month/Year	Code	Name of School		Degree/Diploma/Other			Month/Year Awarded
Street Address and City (Country) of School							State	ZIP Code
Name of Person Who Knew You		Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )

Enter your Social Security Number before going to the next page →

11 YOUR EMPLOYMENT ACTIVITIES

List your employment activities, beginning with the present (#1) and working back 7 years. You should list all full-time work, part-time work, military service, temporary military duty locations over 90 days, self-employment, other paid work, and all periods of unemployment. The entire 7-year period must be accounted for without breaks, but you need not list employments before your 16th birthday. EXCEPTION: Show all Federal civilian service, whether it occurred within the last 7 years or not.

- **Code.** Use one of the codes listed below to identify the type of employment:
  - **1** - Active military duty stations
  - **2** - National Guard/Reserve
  - **3** - U.S.P.H.S. Commissioned Corps
  - **4** - Other Federal employment
  - **5** - State Government (Non-Federal employment)
  - **6** - Self-employment (Include business name and/or name of person who can verify)
  - **7** - Unemployment (Include name of person who can verify)
  - **8** - Federal Contractor (List Contractor, not Federal agency)
  - **9** - Other

- **Employer/Verifier Name.** List the business name of your employer or the name of the person who can verify your self-employment or unemployment in this block. If military service is being listed, include your duty location or home port here as well as your branch of service. You should provide separate listings to reflect changes in your military duty locations or home ports.

- **Previous Periods of Activity.** Complete these lines if you worked for an employer on more than one occasion at the same location. After entering the most recent period of employment in the initial numbered block, provide previous periods of employment at the same location on the additional lines provided. For example, if you worked at XY Plumbing in Denver, CO, during 3 separate periods of time, you would enter dates and information concerning the most recent period of employment first, and provide dates, position titles, and supervisors for the two previous periods of employment on the lines below that information.

Month/Year To Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#1 To Present			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

	Month/Year To Month/Year	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #1)*	Month/Year To Month/Year	Position Title	Supervisor
	Month/Year To Month/Year	Position Title	Supervisor

Month/Year To Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#2 To			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

	Month/Year To Month/Year	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #2)*	Month/Year To Month/Year	Position Title	Supervisor
	Month/Year To Month/Year	Position Title	Supervisor

Month/Year To Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#3 To			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

	Month/Year To Month/Year	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #3)*	Month/Year To Month/Year	Position Title	Supervisor
	Month/Year To Month/Year	Position Title	Supervisor

Enter your Social Security Number before going to the next page →

YOUR EMPLOYMENT ACTIVITIES *(CONTINUED)*

Month/Year Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#4			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

	Month/Year Month/Year To	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #4)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Month/Year Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#5			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

	Month/Year Month/Year To	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #5)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Month/Year Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#6			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

	Month/Year Month/Year To	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #6)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

12 PEOPLE WHO KNOW YOU WELL

List three people who know you well and live in the United States. They should be good friends, peers, colleagues, college roommates, etc., whose combined association with you covers as well as possible the last 7 years. Do not list your spouse, former spouses, or other relatives, and try not to list anyone who is listed elsewhere on this form.

Name **#1**	Dates Known Month/Year Month/Year To	Telephone Number Day Night ( )
Home or Work Address	City (Country)	State / ZIP Code
Name **#2**	Dates Known Month/Year Month/Year To	Telephone Number Day Night ( )
Home or Work Address	City (Country)	State / ZIP Code
Name **#3**	Dates Known Month/Year Month/Year To	Telephone Number Day Night ( )
Home or Work Address	City (Country)	State / ZIP Code

Enter your Social Security Number before going to the next page

13 YOUR SPOUSE

Mark one box to show your current marital status and provide information about your spouse(s) in items a. and/or b.

☐ 1 - Never married	☐ 3 - Separated	☐ 5 - Divorced
☐ 2 - Married	☐ 4 - Legally Separated	☐ 6 - Widowed

a Current Spouse Complete the following about your current spouse only.

Full Name	Date of Birth	Place of Birth *(Include country if outside the U.S.)*	Social Security Number

Other Names Used *(Specify maiden name, names by other marriages, etc., and show dates used for each name)*	Country(ies) of Citizenship

Date Married	Place Married *(Include country if outside the U.S.)*	State

If Separated, Date of Separation	If Legally Separated, Where is the Record Located? City *(Country)*	State

Address of Current Spouse, if different than your current address *(Street, city, and country if outside the U.S.)*	State	ZIP Code

b Former Spouse(s). Complete the following about your former spouse(s), use blank sheets if needed.

Full Name	Date of Birth	Place of Birth *(Include country if outside the U.S.)*	State

Country(ies) of Citizenship	Date Married	Place Married *(Include country if outside the U.S.)*	State

Check one, Then Give Date ☐ Divorced ☐ Widowed	Month/Day/Year	If Divorced, Where is the Record Located? City *(Country)*	State

Address of Former Spouse *(Street, city, and country if outside the U.S.)*	State	ZIP Code	Telephone Number ( )

14 YOUR RELATIVES AND ASSOCIATES

Give the full name, correct code, and other requested information for each of your relatives and associates, living or dead, specified below.

1 - Mother *(first)*	**5** - Foster parent	**9** - Sister	**13** - Half-sister	**17** - Other Relative*
2 - Father *(second)*	**6** - Child *(adopted also)*	**10** - Stepbrother	**14** - Father-in-law	**18** - Associate*
3 - Stepmother	**7** - Stepchild	**11** - Stepsister	**15** - Mother-in-law	**19** - Adult Currently Living With You
4 - Stepfather	**8** - Brother	**12** - Half-brother	**16** - Guardian	

*Code 17 (Other Relative) - include only foreign national relatives not listed in 1 - 16 with whom you or your spouse are bound by affection, obligation, or close and continuing contact. Code 18 (Associates) - include only foreign national associates with whom you or your spouse are bound by affection, obligation, or close and continuing contact.

	Full Name *(If deceased, check box on the left before entering name)*	Code	Date of Birth Month/Day/Year	Country of Birth	Country(ies) of Citizenship	Current Street Address and City *(country)* of Living Relatives	State
☐		1					
☐		2					
☐							
☐							
☐							
☐							
☐							
☐							
☐							
☐							
☐							
☐							

Enter your Social Security Number before going to the next page ⟶

15 CITIZENSHIP OF YOUR RELATIVES AND ASSOCIATES

If your mother, father, sister, brother, child, or current spouse or person with whom you have a spouse-like relationship is a U.S. citizen by other than birth, or an alien residing in the U.S., provide the nature of the individual's relationship to you (Spouse, Spouse-like, Mother, etc.), and the individual's name and date of birth on the first line *(this information is needed to pair it accurately with information in items 13 and 14).*

On the second line, provide the individual's naturalization certificate or alien registration number and use one of the document codes below to identify proof of citizenship status. Provide additional information on that line as requested.

1 - Naturalization Certificate: Provide the date issued and the location where the person was naturalized (Court, City and State).
2 - Citizenship Certificate: Provide the date and location issued (City and State).
3 - Alien Registration: Provide the date and place where the person entered the U S. (City and State).
4 - Other: Provide an explanation in the "Additional Information" block.

Association	Name	Date of Birth *(Month/Day/Year)*
#1		

Certificate/Registration #	Document Code	Additional Information

Association	Name	Date of Birth *(Month/Day/Year)*
#2		

Certificate/Registration #	Document Code	Additional Information

16 YOUR MILITARY HISTORY

	Yes	No
a Have you served in the United States military?		
b Have you served in the United States Merchant Marine?		

List all of your military service below, including service in Reserve, National Guard, and U.S. Merchant Marine. Start with the most recent period of service (#1) and work backward. If you had a break in service, each separate period should be listed.

- **Code.** Use one of the codes listed below to identify your branch of service:
  1 - Air Force **2** - Army **3** - Navy **4** - Marine Corps **5** - Coast Guard **6** - Merchant Marine **7** - National Guard
- **O/E.** Mark "O" block for Officer or "E" block for Enlisted.
- **Status.** "X" the appropriate block for the status of your service during the time that you served. If your service was in the National Guard, do not use an "X": use the two-letter code for the state to mark the block.
- **Country.** If your service was with other than the U.S. Armed Forces, identify the country for which you served.

Month/Year Month/Year	Code	Service/Certificate #	O	E	Status: Active	Active Reserve	Inactive Reserve	National Guard *(State)*	Country
To									
To									

17 YOUR FOREIGN ACTIVITIES

	Yes	No
a Do you have any foreign property, business connections, or financial interests?		
b Are you now or have you ever been employed by or acted as a consultant for a foreign government, firm, or agency?		
c Have you ever had any contact with a foreign government, its establishments (embassies or consulates), or its representatives, whether inside or outside the U.S., other than on official U.S. Government business? *(Does not include routine visa applications and border crossing contacts.)*		
d In the last 7 years, have you had an active passport that was issued by a foreign government?		

If you answered "Yes" to a, b, c, or d above, explain in the space below: provide inclusive dates, names of firms and/or governments involved, and an explanation of your involvement.

Month/Year Month/Year	Firm and/or Government	Explanation
To		
To		

18 FOREIGN COUNTRIES YOU HAVE VISITED

List foreign countries you have visited, except on travel under official Government orders, beginning with the most current (#1) and working back 7 years. (Travel as a dependent or contractor must be listed.)

- Use one of these codes to indicate the purpose of your visit: **1** - Business **2** - Pleasure **3** - Education **4** - Other
- Include short trips to Canada or Mexico. If you have lived near a border and have made short (one day or less) trips to the neighboring country, you do not need to list each trip. Instead, provide the time period, the code, the country, and a note ("Many Short Trips").
- Do not repeat travel covered in items 9, 10, or 11.

	Month/Year Month/Year	Code	Country		Month/Year Month/Year	Code	Country
#1	To			**#3**	To		
#2	To			**#4**	To		

This concludes Part 1 of this form. If you have used Page 9, continuation sheets, or blank sheets to complete any of the questions in Part 1, give the number for those questions in the space to the right:

Enter your Social Security Number before going to the next page →

Standard Form 86
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206-0007
NSN 7540-00-634-4036
86-111

Part 2 OFFICIAL USE ONLY

19 YOUR MILITARY RECORD

Have you ever received other than an honorable discharge from the military? If "Yes," provide the date of discharge and type of discharge below.	Yes	No

Month/Year	Type of Discharge

20 YOUR SELECTIVE SERVICE RECORD

	Yes	No
a Are you a male born after December 31, 1959? If **"No,"** go to 21. If **"Yes,"** go to **b**.		
b Have you registered with the Selective Service System? If **"Yes,"** provide your registration number. If **"No,"** show the reason for your legal exemption below.		

Registration Number	Legal Exemption Explanation

21 YOUR MEDICAL RECORD

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?	Yes	No

If you answered "Yes," provide the dates of treatment and the name and address of the therapist or doctor below, unless the consultation(s) involved only marital, family, or grief counseling, not related to violence by you.

Month/Year	Month/Year	Name/Address of Therapist or Doctor	State	ZIP Code
	To			
	To			

22 YOUR EMPLOYMENT RECORD

Has any of the following happened to you **in the last 7 years?** If **"Yes,"** begin with the most recent occurrence and go backward, providing date fired, quit, or left, and other information requested.	Yes	No

Use the following codes and explain the reason your employment was ended:

1 - Fired from a job
2 - Quit a job after being told you'd be fired
3 - Left a job by mutual agreement following allegations of misconduct
4 - Left a job by mutual agreement following allegations of unsatisfactory performance
5 - Left a job for other reasons under unfavorable circumstances

Month/Year	Code	Specify Reason	Employer's Name and Address *(Include city/Country if outside U.S.)*	State	ZIP Code

23 YOUR POLICE RECORD

For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the court record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

	Yes	No
a Have you ever been charged with or convicted of any felony offense? (Include those under Uniform Code of Military Justice)		
b Have you ever been charged with or convicted of a firearms or explosives offense?		
c Are there currently any charges pending against you for any criminal offense?		
d Have you ever been charged with or convicted of any offense(s) related to alcohol or drugs?		
e In the last 7 years, have you been subject to court martial or other disciplinary proceedings under the Uniform Code of Military Justice? (Include non-judicial, Captain's mast, etc.)		
f In the last 7 years, have you been arrested for, charged with, or convicted of any offense(s) not listed in response to a, b, c, d, or e above? (Leave out traffic fines of less than $150 unless the violation was alcohol or drug related.)		

If you answered "Yes" to a, b, c, d, e, or f above, explain below. Under "Offense," do not list specific penalty codes, list the actual offense or violation (for example, arson, theft, etc.).

Month/Year	Offense	Action Taken	Law Enforcement Authority/Court *(Include City and county/country if outside U.S.)*	State	ZIP Code

Enter your Social Security Number before going to the next page →

24 YOUR USE OF ILLEGAL DRUGS AND DRUG ACTIVITY

The following questions pertain to the illegal use of drugs or drug activity. You are required to answer the questions fully and truthfully, and your failure to do so could be grounds for an adverse employment decision or action against you, but neither your truthful responses nor information derived from your responses will be used as evidence against you in any subsequent criminal proceeding.

		Yes	No
a	Since the age of 16 or in the last 7 years, whichever is shorter, have you illegally used any controlled substance, for example, marijuana, cocaine, crack cocaine, hashish, narcotics (opium, morphine, codeine, heroin, etc.), amphetamines, depressants (barbiturates, methaqualone, tranquilizers, etc.), hallucinogenics (LSD, PCP, etc.), or prescription drugs?		
b	Have you ever illegally used a controlled substance while employed as a law enforcement officer, prosecutor, or courtroom official; while possessing a security clearance; or while in a position directly and immediately affecting the public safety?		
c	In the last 7 years, have you been involved in the illegal purchase, manufacture, trafficking, production, transfer, shipping, receiving, or sale of any narcotic, depressant, stimulant, hallucinogen, or cannabis for your own intended profit or that of another?		

If you answered "Yes" to a or b above, provide the date(s), identify the controlled substance(s) and/or prescription drugs used, and the number of times each was used.

Month/Year To Month/Year	Controlled Substance/Prescription Drug Used	Number of Times Used
To		
To		

25 YOUR USE OF ALCOHOL

	Yes	No
In the last 7 years, has your use of alcoholic beverages (such as liquor, beer, wine) resulted in any alcohol-related treatment or counseling (such as for alcohol abuse or alcoholism)?		

If you answered "Yes," provide the dates of treatment and the name and address of the counselor or doctor below. Do not repeat information reported in response to item 21 above.

Month/Year To Month/Year	Name/Address of Counselor or Doctor	State	ZIP Code
To			
To			

26 YOUR INVESTIGATIONS RECORD

		Yes	No
a	Has the United States Government ever investigated your background and/or granted you a security clearance? If **"Yes,"** use the codes that follow to provide the requested information below. If **"Yes,"** but you can't recall the investigating agency and/or the security clearance received, enter **"Other"** agency code or clearance code, as appropriate, and **"Don't know"** or **"Don't recall"** under the **"Other Agency"** heading, below. If your response is **"No,"** or you don't know or can't recall if you were investigated and cleared, check the **"No"** box.		

Codes for Investigating Agency
1 - Defense Department **4** - FBI
2 - State Department **5** - Treasury Department
3 - Office of Personnel Management **6** - Other *(Specify)*

Codes for Security Clearance Received
0 - Not Required **3** - Top Secret **6** - L
1 - Confidential **4** - Sensitive Compartmented Information **7** - Other
2 - Secret **5** - Q

Month/Year	Agency Code	Other Agency	Clearance Code	Month/Year	Agency Code	Other Agency	Clearance Code

		Yes	No
b	To your knowledge, have you ever had a clearance or access authorization denied, suspended, or revoked, or have you ever been debarred from government employment? If "Yes," give date of action and agency. Note: An administrative downgrade or termination of a security clearance is not a revocation.		

Month/Year	Department or Agency Taking Action	Month/Year	Department or Agency Taking Action

27 YOUR FINANCIAL RECORD

		Yes	No
a	In the last 7 years, have you filed a petition under any chapter of the bankruptcy code (to include Chapter 13)?		
b	In the last 7 years, have you had your wages garnished or had any property repossessed for any reason?		
c	In the last 7 years, have you had a lien placed against your property for failing to pay taxes or other debts?		
d	In the last 7 years, have you had any judgments against you that have not been paid?		

If you answered **"Yes"** to a, b, c, or d, provide the information requested below:

Month/Year	Type of Action	Amount	Name Action Occurred Under	Name/Address of Court or Agency Handling Case	State	ZIP Code

Enter your Social Security Number before going to the next page ⟶

28 YOUR FINANCIAL DELINQUENCIES	Yes	No
a In the last 7 years, have you been over 180 days delinquent on any debt(s)?		
b Are you currently over 90 days delinquent on any debt(s)?		

If you answered **"Yes"** to a or b, provide the information requested below:

Incurred Month/Year	Satisfied Month/Year	Amount	Type of Loan or Obligation and Account Number	Name/Address of Creditor or Obligee	State	ZIP Code

29 PUBLIC RECORD CIVIL COURT ACTIONS	Yes	No
In the last 7 years, have you been a party to any public record civil court actions not listed elsewhere on this form?		

If you answered "Yes," provide the information about the public record civil court action requested below.

Month/Year	Nature of Action	Result of Action	Name of Parties Involved	Court *(Include City and county/country if outside U.S.)*	State	ZIP Code

30 YOUR ASSOCIATION RECORD	Yes	No
a Have you ever been an officer or a member or made a contribution to an organization dedicated to the violent overthrow of the United States Government and which engages in illegal activities to that end, knowing that the organization engages in such activities with the specific intent to further such activities?		
b Have you ever knowingly engaged in any acts or activities designed to overthrow the United States Government by force?		

If you answered "Yes" to a or b, explain in the space below.

Continuation Space

Use the continuation sheet(s) (SF86A) for additional answers to items 9, 10, and 11. Use the space below to continue answers to all other items and any information you would like to add. If more space is needed than is provided below, use a blank sheet(s) of paper. Start each sheet with your name and Social Security Number. Before each answer, identify the number of the item.

After completing Parts 1 and 2 of this form and any attachments, you should review your answers to all questions to make sure the form is complete and accurate, and then sign and date the following certification and sign and date the release on Page 10.

Certification That My Answers Are True

My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of title 18, United States Code).

Signature *(Sign in ink)*	Date

Enter your Social Security Number before going to the next page ⟶

Standard Form 86
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

Form approved:
OMB No. 3206-0007
NSN 7540-00-634-4036
86-111

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

I Authorize any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain any information relating to my activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record information, and financial and credit information. I authorize the Federal agency conducting my investigation to disclose the record of my background investigation to the requesting agency for the purpose of making a determination of suitability or eligibility for a security clearance.

I Understand that, for financial or lending institutions, medical institutions, hospitals, health care professionals, and other sources of information, a separate specific release will be needed, and I may be contacted for such a release at a later date. Where a separate release is requested for information relating to mental health treatment or counseling, the release will contain a list of the specific questions, relevant to the job description, which the doctor or therapist will be asked.

I Further Authorize any investigator, special agent, or other duly accredited representative of the U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, the Defense Investigative Service, and any other authorized Federal agency, to request criminal record information about me from criminal justice agencies for the purpose of determining my eligibility for access to classified information and/or for assignment to, or retention in a sensitive National Security position, in accordance with 5 U.S.C. 9101. I understand that I may request a copy of such records as may be available to me under the law.

I Authorize custodians of records and sources of information pertaining to me to release such information upon request of the investigator, special agent, or other duly accredited representative of any Federal agency authorized above regardless of any previous agreement to the contrary.

I Understand that the information released by records custodians and sources of information is for official use by the Federal Government only for the purposes provided in this Standard Form 86, and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for five (5) years from the date signed or upon the termination of my affiliation with the Federal Government, whichever is sooner. Read, sign and date the release on the next page if you answered "Yes" to question 21.

Signature *(Sign in ink)*	Full Name *(Type or Print Legibly)*		Date Signed
Other Names Used			Social Security Number
Current Address *(Street, City)*	State	ZIP Code	Home Telephone Number *(Include Area Code)*
			( )

Page 10

Standard Form 86
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

Form approved:
OMB No. 3206-0007
NSN 7540-00-634-4036
86-111

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

Instructions for Completing this Release

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position with the Federal government which requires access to classified national security information or special nuclear information or material. As part of the clearance process, **I hereby authorize** the investigator, special agent, or duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain the following information relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgment or reliability, particularly in the context of safeguarding classified national security information or special nuclear information or material?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 86 and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

Signature *(Sign in ink)*	Full Name *(Type or Print Legibly)*		Date Signed
Other Names Used			Social Security Number
Current Address *(Street, City)*	State	ZIP Code	Home Telephone Number *(Include Area Code)* ( )

CONSENT TO UNDERGO POLYGRAPH EXAMINATION

I, _____, have been asked to undergo polygraph examination by Special Agent _____, DIS, regarding national security matters. I understand that:

a. The polygraph examination is voluntary and I must consent in writing prior to undergoing the examination.
b. Adverse action will not be taken against me based solely on a refusal to undergo this examination, and any refusal will not be recorded in my personnel file.
c. Refusal to undergo polygraph examination does not preclude security investigation by other means.
d. The examiner will provide an explanation of the polygraph instrument and review all test questions prior to the examination.
e. The examination area contains the following listening / monitoring devices: (two-way mirror) (camera) (audio monitoring-listening device). I understand this examination will be recorded and or observed.
f. This consent form does not constitute a waiver of my Constitutional rights against self incrimination.
g. I may consult with a legal counsel to answer questions in conjunction with this polygraph examination.

I UNDERSTAND THE ABOVE PROVISIONS AND FREELY AND VOLUNTARILY CONSENT TO UNDERGO POLYGRAPH EXAMINATION. NO THREATS HAVE BEEN MADE OR PROMISES EXTENDED TO ME TO OBTAIN MY PARTICIPATION IN THIS EXAMINATION.

DATE	SIGNATURE OF EXAMINEE
DATE AND TIME	SIGNATURE OF POLYGRAPH EXAMINER
SIGNATURE OF WITNESS	

DIS Form 181, Jul 91

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual — Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable

312-102

STANDARD FORM 312 (Rev. 1-00
Prescribed by NARA/ISOO
32 CFR 2003. E.O. 12958

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		**ACCEPTANCE**	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

*U.S. Government Printing Office: 2001-683-003/24011