

FINAL REPORT AND RECOMMENDATIONS

FEDERAL EMERGENCY MANAGEMENT AGENCY

SECURITY PRACTICES BOARD OF REVIEW



November 1992

FINAL REPORT AND RECOMMENDATIONS

FEDERAL EMERGENCY MANAGEMENT AGENCY

SECURITY PRACTICES BOARD OF REVIEW

November 1992



NOV 12 1992

The Honorable Wallace E. Stickney
Director, Federal Emergency
Management Agency
500 C Street, S.W.
Washington, D.C. 20472

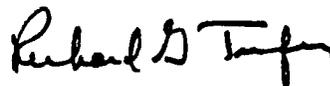
Dear Mr. Stickney:

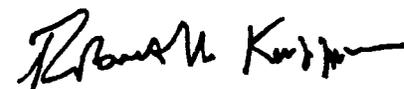
It has been an honor and privilege to have served on the Security Practices Board of Review, which you established in May 1992 to study and recommend actions concerning the personnel security practices at the Federal Emergency Management Agency.

The enclosed final report and unanimous recommendations contain the results of our work.

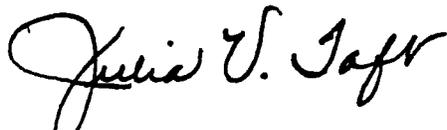
Very truly yours,


Andrew J. Goodpaster


Richard G. Trefry, Chairman


Robert Kupperman


Peter F. Dabrowski


Julia V. Taft


Lorri J. Jean

Enclosures

TABLE OF CONTENTS

Preface	3
I. Board Charter	5
II. Board Membership	6
III. Board Activities	7
IV. Discussion:	
Introduction	8
Excessive Number of Security Clearances	9
The Security Labyrinth	10
Homosexuality	13
V. Observations for FEMA Management	16
VI. Recommendations	18
VII. Tabs:	
A. Charter	
B. Board Appearances	
C. Letter from the Board Chairman to all FEMA Employees	
D. The Personnel Security Process	
E. Personnel Security Authorities	
F. Sexual Orientation: Security Criteria, Vulnerability, Secrets	
G. DoD/NISP Criteria: Sexual Conduct/Vulnerability	

PREFACE

In a press release dated May 28, 1992, The Honorable Wallace E. Stickney, Director of the Federal Emergency Management Agency (FEMA), stated that he had requested six distinguished individuals to serve on a board of review to study and recommend appropriate actions concerning the personnel security practices of the Agency.

During the past three years, several events occurred that led the Director to review personnel security practices:

- The change in the external threat to the United States, which reduced the chances for a Soviet nuclear holocaust, has affected FEMA's requirements.
- Changes in social mores and actions directed by courts and other agencies have evolved that affected personnel security practices.
- The Office of Personnel Management (OPM) completed an appraisal of the FEMA personnel security and suitability program in 1989. Actions to adopt the recommendations of this appraisal have been ongoing. Most have been accomplished.
- An assessment of FEMA personnel security clearance functions by the FEMA Inspector General initiated several additional actions.

All of these actions, plus some notoriety and allegations in the spring of 1992, involving security practices and homosexuality, led to the decision to create an advisory board to review FEMA personnel security practices.

The Board was charged to review the current practices and operations of the FEMA Security Office, as well as the number and types of clearances required to carry out the various missions of the Agency. The Board was requested to offer recommendations which would result in updated, more efficient, or improved operations. Of particular concern were observations derived from the report of the FEMA Inspector General by the

Director indicating, "that our Office of Security may be operating under out-outmoded procedures . . . ," and concern that "FEMA security practices reflect not only contemporary security standards but the nature of FEMA's mission." This Board reviewed statutes, Executive orders, as well as directives derivative from agencies that FEMA supports, to determine if FEMA was in compliance.

The specific tasks imposed on the Board are reflected in its Charter.

I. BOARD CHARTER

The Charter of the Security Practices Board of Review (herein referred to as the Board) was presented to the Board on Friday, June 26, 1992. Copies of the proposed Charter had been made available to the members of the Board prior to the meeting. Minor changes for clarification were incorporated by the Board with the approval of the Director. A final, corrected copy of the Charter is attached at Tab A.

II. BOARD MEMBERSHIP

General Andrew J. Goodpaster, United States Army (retired), formerly Supreme Allied Commander Europe, Superintendent of the United States Military Academy at West Point, and the Staff Secretary and Defense Liaison Officer under President Eisenhower. He is now Chairman of the Atlantic Council of the United States.

Lieutenant General Richard G. Trefry, United States Army (retired), a West Point graduate, a former Military Assistant to President Bush, and Director of the White House Military Office. He served six years as Inspector General of the Army. (He was elected by its members as Chairman of the Federal Emergency Management Agency Security Practices Board of Review at the June 26, 1992, meeting.)

Robert Kupperman, Center for Strategic and International Studies, and a consultant on national security matters located in Washington, D.C. He has had a distinguished career in government on national and international levels.

Julia V. Taft, a former director of the United States Office of Foreign Disaster Assistance, Agency for International Development, and recipient of several federal awards: a White House Fellowship; the Presidential End Hunger Award; and the Arthur Flemming Award, as one of the top 10 men and women in Federal service.

Lorri L. Jean, an attorney, now serving as Deputy Regional Director at FEMA's San Francisco Regional Office. An honors graduate from the Georgetown University Law Center, she became FEMA Associate General Counsel for General Law in 1988 and was promoted to her current position the next year. Ms. Jean has been recognized for her efforts at promoting equity in federal service for all employees.

Colonel Peter F. Dabrowski, United States Army, is currently assigned as Chief of the Department of Defense Military Support Liaison Office to FEMA. Prior to this assignment at FEMA, Col. Dabrowski was Chief of Security, Plans and Operations, for the Army's 4th Transportation Command in Germany.

III. BOARD ACTIVITIES

The Board held open meetings on June 26; July 24; August 6, 25, 26, and 28; September 4 and 23; and November 12, 1992. The Board met in a closed session for approximately one hour on June 26 for the purpose of hearing a classified briefing.

A list of individuals who appeared and presented material to the Board and a list of those who attended and participated are attached at Tab B.

At the June 26 meeting, the Board directed that a letter from the Board Chairman to all employees of the Federal Emergency Management Agency (FEMA) be sent requesting any comments or observations concerning security practices within FEMA. A copy of the dispatched letter is attached at Tab C. There were 12 replies. Writers were asked to sign their letters with the promise that every effort would be made to preserve the anonymity of the writer. The Board has been conscientious in carrying out that promise.

IV. DISCUSSION

Introduction

Any review of FEMA's personnel security program must consider that the world has changed drastically in the past three years. The original Executive order establishing the personnel security program for the Federal Government was promulgated in 1953 during the first administration of President Eisenhower. At that time, the world faced the threat of militant and aggressive communism, and, with it, the United States experienced the traumatic environment that is commonly referred to as "McCarthyism." The geopolitical tenor in the world has evolved from that of two superpowers with their client and satellite states to that of one superpower and a series of states involved in a search for stability and development. This is complicated by a multitude of ethnic, nationalist and sectarian disputes and conflicts. Heavily armed and aggressive third-world actors contribute to the instability. Change is so accelerated that time appears to be compressed.

The Board was struck by the complexity of laws and regulations that have evolved over the last 40 years to meet the threats to national security. Because of fundamental geopolitical changes in the nature of the threat, the Board recommends that the time has come for a thorough review, in all departments of the government, of procedures and criteria for personnel security.

FEMA provides an excellent example of an organization with once onerous security requirements that the Board believes are no longer relevant, or in anyway comparable to previous times. Moreover, a review of the FEMA mission statement by the Board disclosed that although no requirement for any classified activity is stated in explicit terms, some elements of the mission do, in fact, require security protection and access to classified information. The Board recommends that the FEMA Organization and Functions Manual of August 1988 be revised to accurately describe the actual personnel security assignments and delegations within the Agency.

Excessive Number of Security Clearances

As far as the Board could determine, there are three areas that involve FEMA in present day classified activities and, hence, national security issues. They are national preparedness, industrial preparedness and responses to the consequences of terrorist acts. The Board believes that the security requirements of FEMA in these areas are to a large extent a function of exposure to classified plans, programs, and other information generated by other federal agencies, rather than internally-generated security activities. The Board was informed that of 2,604 FEMA employees, 1,501 possessed top secret clearances, and 381 possessed secret clearances. Discussions with operators in agencies requiring security clearances have led the Board to recommend that the number of clearances in the Agency be sharply reduced with a goal of reaching approximately 300. Additional reductions may be possible after a more complete analysis. Any reduction must be accompanied by a program to educate FEMA employees on the revised personnel security policies and to explain in detail the reasons for the reductions in the number of clearances.

The reduction of clearances to this level would go far toward removing a culture that is all too common throughout the government, e.g., that a security clearance is important for a successful career. The Board was provided testimony of a pervasive belief by FEMA employees that a security clearance is essential for career advancement. The Board believes that security clearances within FEMA were designed to meet legitimate security requirements, and did so, but that these requirements also set a social standard throughout the Agency. The reduction proposal would have the effect of reducing or eliminating the culture.

The phenomenon is not new. A 1985 report to the Secretary of Defense by the Commission to Review the Department of Defense (DoD) Security Policies and Practices, entitled "Keeping the Nation's Secrets" and commonly called "The Stilwell Report," made similar observations regarding the number of clearances. The experience of the members of this Board, who are knowledgeable in the workings of the DoD and other agencies in the government, confirmed the existence of a belief that a security clearance was necessary for advancement. The Board

recommends that the Executive and Legislative Branches of the Federal Government take joint action to bring a greater degree of order and reason to the extensive requirements for security clearances. The Board also notes that representatives from the Office of Personnel Management (OPM), in testimony before the Board, also expressed a belief that there are an excessive number of security clearances in the Federal Government. The FEMA Inspector General, as a result of his 1991 assessment, has expressed the same opinion with respect to FEMA.

The Security Labyrinth

Much of the security clearance and classification process at FEMA is derived from the requirements and cultures of the DoD and Department of Energy. As a result, FEMA must comply with the security requirements of these departments. Not only does this create an administrative burden when applied to so many in FEMA, but the cost of investigations for security is disproportionate in relation to funds currently appropriated by Congress. The costs of initial investigations run approximately from \$1,700 to \$3,000 per person. The Board was informed that because of budget limitations, funds frequently are not available to conduct periodic personnel security investigations. The Board was informed that the expected security budgetary shortfall for next year would probably exceed \$1 million. This does not augur well for a disciplined personnel security system.

A further concern of the Board relates to reported attempts, made in the past, to use the personnel security system improperly to expedite the removal of individuals from FEMA. Hypothetically, an unproductive worker could be accused of conduct or behavior that could prompt revocation of the individual's security clearance. This leverage could then provide the means for transferring or otherwise terminating the employment of the individual rather than pursuing the more complex process of a performance-based, adverse personnel action.

The statutes, Executive orders, regulations, and directives governing the personnel security system are so complex that they form an administrative labyrinth. Consequently, management is often at a loss to

comprehend just exactly what is intended or needed. There is little or no orientation or instruction on this matter provided to the senior leadership upon assuming positions in the Agency. Although the Board is composed of six individuals, all with extensive service within the government, it still took two full days of surgical dissection to attempt to understand the August 1991 versions of the Federal Personnel Manual, Chapter 731 and Chapter 732, as well as applicable Executive orders and statutes.

The Board recommends that simplified and understandable instruction in personnel security processes be prepared and presented to all civilian employees of the Federal Government. In addition, managers at all levels should be required to receive the necessary instruction that would ensure their competence and understanding in this vital matter. The Board also recommends that the FEMA leadership at all levels participate more actively in the personnel security program. The Board also believes that the system is so complex that its processes cannot be executed with expectation of equity to the individual or effective provision for national security. The program has become highly bureaucratic and is vulnerable to critics, however competent or ignorant, both in and out of government. After extensive review of this program, the Board prepared a comprehensive flowchart (Tab D) illustrating the steps required in obtaining suitability determinations and security clearances. The Board suspects its flowcharts and analyses may provide the most comprehensive description of the personnel security process extant in the Federal Government today.

An additional set of flowcharts and descriptive materials is enclosed under Tab E. It contains eight enclosures consisting of various reference materials on "Personnel Security Authorities." An introductory enclosure lists and identifies each enclosure and includes certain footnote information on the location of cross-referenced information.

- Enclosure 1 is a schematic diagram for Executive Order (EO) 10450. It outlines the statutory authorities that support the order and the OPM regulation. It also separates the functions and responsibilities of the OPM and agency heads with respect to the creation, execution, and

regulation of the Federal Government's personnel security program. The personnel security program in FEMA is governed by these authorities.

- Enclosure 2 is a schematic diagram for Executive Order 12356. It identifies the legal basis for this order, which governs the security classification and clearance system in the Federal Government. The diagram also separates various functional responsibilities and emphasizes those actions required of all agencies, including FEMA. Specific implementing regulations of FEMA are also identified.
- Enclosure 3 is a chart reflecting the various rule-making authorities relied upon by OPM to promulgate both the former and current versions of its personnel security regulations which are codified in Title 5 of the Code of Federal Regulations (CFR), Parts 721, 732, and 736.
- Enclosure 4 is a series of footnotes and cross-references that identify and summarize various statutory and Executive order authorities mentioned in Enclosures 1, 2, and 3. It also refers to more detailed descriptions in Enclosure 5.
- Enclosure 5 is a Synopsis of Personnel Security Authorities. It illustrates the variety and complexity of the Federal Government's personnel security programs.
- Enclosure 6 is a complete copy of Executive Order 10450, as amended.
- Enclosure 7 is a complete copy of Executive Order 12356.
- Enclosure 8 contains the most recent OPM regulations on personnel suitability, national security positions, and investigations (Title 5 CFR, Parts 731, 732, and 736).

The Board is convinced that no one will ever understand the current personnel security program until there is a capability to decipher the mysteries of the arcane jungle that is the personnel security program in government today. During the meetings of the Board there were repeated revision, discussion, contradiction, confusion, and reference to other

equally applicable terminology or regulations. It was also apparent that the confidence and morale of FEMA employees are noticeably low regarding the personnel security program.

Everyone wants to reduce the number of security clearances, thereby reducing the number of investigations. It must be realized, however, that even if all security clearances were eliminated, the number of background investigations could remain nearly the same. The reason is that positions of "public trust," i.e., those designated as moderate or high risk, can require basically the same investigation as for security clearances. This fact is not widely understood in or out of government. Therefore, in order to reduce the number of background investigations, the Board recommends that FEMA also minimize the number of "public trust" positions.

The Board recommends, as a matter of priority, that the current draft of the FEMA Personnel Security Manual be revised to include all applicable statutes, Executive orders, practices, instructions, and regulations in a format that is readable and understandable to the average person. (This recommendation is also applicable to personnel security manuals throughout the Federal Government.)

Homosexuality

The Board recognizes that the primary impetus for its review came from allegations regarding improper actions within the Agency relating to homosexual employees. The Board at its initial meeting agreed that it should not involve itself in attempting to determine the specific rights or wrongs of individual cases but rather should review generic allegations at a policy level. Accordingly, individuals with personal grievances were not interviewed.

There is no question that in the matter of homosexual employees the requirements of outside agencies have been applied to FEMA. While these requirements may be legally supportable, they do not appear to reflect the findings of recent studies, policies, or decisions involving heterosexual or homosexual conduct.

The Board understands that the current position of most government departments and agencies is that announced homosexual conduct is not grounds for denying or revoking a security clearance. As a matter of interest and research, attached at Tab F are two memoranda addressing this matter prepared by Ms. Lorri L. Jean, a member of the Board.

Tab G includes enclosures that compare the two most significant provisions in both the existing and/or proposed personnel security criteria of DoD (App. I, DoD 5200.2-R) and a joint industrial-government security practices group (Annex A, National Industrial Security Program (NISP) Guidelines). These criteria may continue to have a significant influence on current and future personnel security practices involving homosexuals.

The Board was also impressed by a September 1991 report, "Homosexuality and Personnel Security," which was prepared by Theodore R. Sarbin, Ph.D., and published by the Defense Personnel Security Research and Education Center (PERSEREC) in Monterey, California. PERSEREC is a Department of Defense organization that reports directly to the Deputy Assistant Secretary of Defense for Counter-Intelligence and Security Counter-Measures. This study found that homosexuality should not be grounds for denial or revocation of a security clearance. Nevertheless, there are indications of continuing concern within government agencies that unannounced ("in the closet") homosexuals may be subject to undue coercion or blackmail. After careful consideration, the Board has concluded that the evidence indicates that homosexuals, "in or out of the closet," are no more vulnerable to coercion or blackmail than heterosexuals. The Board found the PERSEREC study particularly compelling. The following excerpt is provided from the study, page 30:

"The PERSEREC data bank currently includes 117 cases of American citizens who between 1945 and the present committed or attempted to commit espionage. Only six have been identified as homosexuals. Their motives appear to be the same as for persons not identified as homosexuals:

primarily money, secondarily resentment. All were volunteers except one, who was recruited as an accomplice by a heterosexual friend. None was a target of blackmail although one offender claimed to have been coerced."

Accordingly, the Board recommends that no agency of the Federal Government deny, on the basis of potential vulnerability, security clearances to civilian employees of the Federal Civil Service (or applicants thereto) solely on account of their homosexuality or sexual orientation. (The Board does not refer to members of the military services, noting that this is a far more complex matter beyond the purview of the Board.)

Moreover, the Board further recommends that Federal regulations, standards, guidelines, and other personnel security directives be revised to make it inappropriate and unnecessary, in the absence of any other security concerns, for government security personnel to require any Federal civilian employee or potential civilian employee to publicize his/her sexual orientation or that of any other person as a condition of employment within the Federal Civil Service or for obtaining a Federal Government security clearance.

The Board does note, however, that in either heterosexual or homosexual relationships within the "chain of command" of an office or an organization, such relationships are divisive and corrosive in their effect. The principle of the senior-subordinate relationship in any organization requires the exercise of all the talents of leadership and management. Any relationship that violates these principles is harmful to effective performance.

V. OBSERVATIONS FOR FEMA MANAGEMENT

The Board believes that the personnel security system in the Federal Government, including that of FEMA, is overly complex, arcane, and needs to be brought into the realities of the 1990's. The Board believes strongly that the problems in the system should not be attributed to security personnel in particular, either as individuals or in groups of individuals in FEMA, or elsewhere in the civil service. They are required to administer a bureaucratic nightmare.

In truth, the leadership (or the management) of any federal agency may be the greatest victims of the system. Because of the complexity of the system, security personnel have largely been put on their own and have operated under a pervasive and severe threat in case of failure. Their superiors likewise have found themselves faced with a complex system that breeds controversy and threatens instantaneous, intense political and public attacks based on any perceived personal injustice. As a result, security personnel work without adequate guidance to maintain a system that breeds overreaction. Management has little incentive to tackle the sleeping bear. The discipline in the system comes not from leadership or management policies but rather from a reactive, protective, inbred process. The personnel security system throughout the entire government needs a comprehensive overhaul. There are no villains except those who accept the status quo or find the system too difficult to even attempt to change.

It is the view of the Board that many of the problems in FEMA involving the administration of the personnel security program could be reduced or eliminated by assuring that the individual serving as Deputy or Chief of Staff to the Director of FEMA be required to be thoroughly knowledgeable in personnel security and related staff management procedures. Political appointees with little practical experience within the federal bureaucracy find difficulty in coping with a program as complex as personnel security procedures.

The Board feels very strongly that the problems that it found within FEMA's personnel security program are no different than those found in other federal agencies. As mentioned earlier, the 1985 Stilwell Report found similar problems at DoD. The Board's feelings regarding the pervasiveness of the personnel security problems throughout the Federal Government were reinforced when the members of the Board were provided copies of a Report by the Committee on Government Operations of the House of Representatives, dated August 22, 1992, entitled "Investigating the Investigators: Justice Department Background Reviews Break Down" (House Report 102-854).

The Board noted many similarities in the types of problems uncovered in this report and those found by this Board to include: misuse of waivers; an unmanageable reinvestigation backlog; confusion within the Federal Government regarding the standards for security clearances and suitability determinations; and failure to insure that standards established for employment at the Justice Department were met.

The Board believes that such similar findings reinforce its recommendations that the time has come for a Government-wide review of personnel security practices. The entire system needs to be streamlined and simplified.

Although the Charter of the Board was limited to looking at personnel security practices in FEMA, the Board recommends that the Director forward the results of this analysis to the attention of higher authority for government-wide consideration and action.

VI. RECOMMENDATIONS

The following is a complete list of recommendations that were sequentially extracted from the report and from Tab D. The page numbers in parentheses after each recommendation indicate where it can be found within the text.

1. That all departments of the Federal Government, including FEMA, conduct a thorough review of procedures and criteria for personnel security (page 8).
2. That the FEMA Organization and Functions Manual of August 1988 be revised to accurately describe actual personnel security assignments and delegations within FEMA (page 8).
3. That the number of clearances in the Agency be sharply reduced with a goal of reaching approximately 300, and that further analysis be conducted to determine the feasibility of making further reductions (page 9).
4. That the Executive and Legislative Branches of the Federal Government take joint action to bring a greater degree of order and reason to the extensive requirements for security clearances (page 9).
5. That simplified and understandable instruction in personnel security processes be prepared and presented to all civilian employees of the Federal Government, and that managers at all levels be required to receive the necessary instruction that would ensure their competence and understanding in this vital matter. Training should include instruction on determining risk and sensitivity levels and security clearance requirements (page 11).
6. That FEMA leadership at all levels participate more actively in the personnel security program (page 11).
7. That FEMA minimize the number of "public trust" positions in order to reduce the number of background investigations (page 13).

8. That, as a matter of priority, the current draft of the FEMA Personnel Security Manual be revised to incorporate all applicable statutes, Executive orders, practices, instructions, and regulations in a format that is readable and understandable to the average person. (This recommendation is also applicable to personnel security manuals throughout the Federal Government) (page 13).

9. That no agency of the Federal Government deny, on the basis of potential vulnerability, security clearances to civilian employees of the Federal Civil Service (or applicants thereto) solely on account of their homosexuality or sexual orientation (page 15).

10. That Federal regulations, standards, guidelines, and other personnel security directives be revised to make it inappropriate and unnecessary, in the absence of any other security concerns, for government security personnel to require any federal civilian employee or potential civilian employee to publicize his/her sexual orientation or that of any person as a condition of employment or for obtaining a Federal Government security clearance (page 15).

11. That any individual chosen to serve as the Deputy Director or the Chief of Staff to the Director of FEMA be required to be thoroughly knowledgeable in personnel security and related staff management procedures (page 16).

12. That the Director of FEMA forward the results of the Board's analysis to the attention of higher authority for government-wide consideration and action (page 17).

The following recommendations relate to the Board's study of the suitability and security clearance processes as reflected in Tab D:

13. That a FEMA senior executive carefully and continually review all positions, especially those designated as "public trust" or national security, to ensure that they are assigned the appropriate risk and/or sensitivity levels in accordance with the new risk and sensitivity level designation system and FEMA requirements for security clearances (page D-3).

14. That, as the requirements for security clearances within FEMA are reduced, any removal of an individual's clearance must be accomplished in a nonprejudicial manner (page D-3).
15. That FEMA develop and conduct a program to educate its employees on the revised personnel security clearance policies and explain in detail the reasons for the reductions in the number of clearances (page D-3).
16. That FEMA modify its mission statement to include requirements for classified activities and review its "organization and functions" manual and any personnel security regulations to ensure that they are consistent and accurately describe all personnel security requirements and assignments (page D-3).
17. That FEMA prepare an internal guidance document to ensure that its risk and sensitivity level criteria and security clearance requirements are described and implemented correctly (page D-5).
18. That FEMA consult appropriate authorities to resolve an open issue as to whether or not a waiver of a pre-appointment investigation is permitted for a "public trust" position (page D-6).
19. That FEMA modify its recent delegation of suitability determination authority so that the Office of Human Resources Management (HRM) would have sole responsibility for making all basic, i.e., Part 731, suitability determinations for all positions (page D-7).
20. That the Director of FEMA continue to have ultimate responsibility for making all final determinations involving the denial, suspension or revocation of security clearances (page D-8).
21. That FEMA management take immediate action to correct the problem of having periodic reinvestigations, i.e., investigations required for periodic updates of security clearances, being postponed due to lack of funds, and to bring this matter to the attention of the highest security authorities within the Administration and Congress (page D-9).

22. That FEMA consider providing in-house legal assistance in those cases where an investigation of a FEMA employee leads to a determination of unsuitability and/or the denial, suspension, or revocation of a security clearance (page D-9).

23. That the terminology used to describe the various steps in the personnel security process be clarified. The Board found the following terms more understandable than some of the terms currently in use (page D-11):

- a. Requirement
- b. Application
- c. Initiation
- d. Investigation
- e. Evaluation
- f. Recommendation
- g. Determination

24. That FEMA management specifically assign responsibility for each step (a through g) in the personnel security process to either management or staff, with the Office of Security only providing staff recommendations to FEMA management in these important matters and the Director, FEMA, making all final decisions, i.e., all appeal determinations (page D-11).

25. Finally, the Board recommends that FEMA use the contents of Tab D as the basis for detailed and explicit instructions on the personnel security systems and practices within FEMA (page D-12).

A

**Federal Emergency Management Agency
Security Practices Board of Review**

CHARTER

A. Official Designation

This is the Charter for the Federal Emergency Management Agency (FEMA) Security Practices Board of Review (herein "Board").

B. Objective and Scope

The purpose of the Board shall be to conduct a complete review of FEMA's personnel security program and FEMA's compliance with Executive Orders 10450 and 12356, and to make appropriate recommendations to the Director, FEMA, for development, changes, revocations of FEMA procedures and any other actions deemed necessary in order to ensure compliance with those Executive orders and to ensure that Constitutional due process requirements for placement in or removal from National Security positions responsibilities are met.

C. Duration

The Board shall submit its recommendations by September 11, 1992, and shall terminate on December 31, 1992.

D. Authority

The Board shall report solely to the Director of FEMA. The FEMA Security Practices Board of Review is established pursuant to my authority of Director of FEMA under Executive Orders 10450, 12148, 12356, and 12656. The operations of this Board are subject to the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2.

E. Organization

The Board shall organize its members and conduct its operations in accordance with own procedures developed by the Board. Minority reports on issues are encouraged if necessary but, to the extent possible,

consensus recommendations shall be given in order to expedite their consideration and possible adoption. The Director shall furnish appropriate staff upon request by the Board Chair who shall be selected by the Board. The Director shall provide a support staff executive from current FEMA employees.

F. Objectives and Scope

The Board shall have complete and full authority to make any and all recommendations to the Director without prior review from any persons or organizations within or outside of FEMA. The Board shall conduct its activities and transmit its final recommendations by September 11, 1992. It may submit interim findings and recommendations to the Director as it may deem appropriate. While it is the mandate of the Board to operate solely in an advisory capacity and focus on any issues involving FEMA's security operations that it finds appropriate, the following concerns and requests of the Director shall be included by the Board in its areas of concerns and recommendations:

1. Whether FEMA's security clearance procedures are appropriate from a legal and policy standpoint in light of current world situation and other developments pertinent to the FEMA mission.
2. Whether the security mission of FEMA is adequately staffed and positioned within FEMA; whether it is subject to adequate supervisory and legal review.
3. Whether personnel within FEMA are accorded all Constitutional and statutory rights in personnel security determinations.
4. Whether currently utilized criteria are proper factors for consideration in granting suspensions or revoking of access to classified information or assignment to a national security position, and, if so, under what conditions and control mechanisms and whether additional privacy concerns should be directly addressed in FEMA's security operations while still ensuring reasonably needed National Security protection.

5. Whether recommendations provided by the Inspector General in the course of his most recent inspection of the Security Office are being properly implemented.

G. Operational Costs

The estimated costs of operation of the Committee is \$25,000.

H. Estimated Number and Frequency of Meetings

The Committee shall meet at least three times, but can meet as frequently as the members determine is necessary.

I. Termination

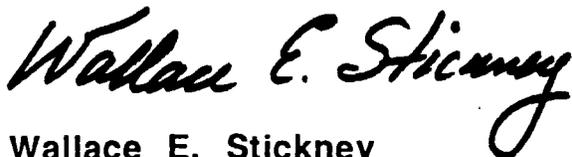
The Board will terminate December 31, 1992.

J. Date of Filing of Charter

The Charter was filed with the General Services Administration on June 2, 1992, and has been filed with the standing committees of the Senate and of the House of Representatives, having legislative jurisdiction of FEMA and the Library of Congress.

Dated: June 17, 1992

As Amended June 26, 1992



Wallace E. Stickney
Director

BOARD APPEARANCES

The following individuals were interviewed by or presented materials to the members of the FEMA Security Practices Board of Review:

William C. Coe

Advisory Committee Management Officer
Office of Administrative Support, FEMA

Richard S. Eligan, Jr.

Chief, Personnel Security Division
Office of Security, FEMA

G. Clay Hollister

Deputy Assistant Associate Director, Office of Operations
National Preparedness Directorate, FEMA

John R. Lilley, II

Director, Office of Security, FEMA

Antonio Lopez

Associate Director, National Preparedness Directorate, FEMA

Kenneth McGloughlin

Contract Adjudicator, M.V.M. Corporation

Peter R. Nelson

Deputy Director for Personnel Security, Office of the Deputy
Assistant Secretary of Defense for Counterintelligence
and Security Countermeasures

Kathryn L. Newman

Deputy General Counsel, FEMA

Dennis Owens

Deputy Director, Office of Human Resources Management, FEMA

Grant C. Peterson

Associate Director
State and Local Programs and Support Directorate, FEMA

Frances A. Sclafani

Associate Director, Investigations Group
Office of Personnel Management

Ms. Sclafani was accompanied by:

John J. Lafferty

Deputy Associate Director, Investigations Group,

Robert J. Longo

Chief, Investigation Appraisal Assistance Branch
Investigations Evaluation Division, Office of Federal
Investigations

Wallace E. Stickney

Director, Federal Emergency Management Agency

William C. Tidball

Assistant Inspector General for Inspections, FEMA

(Currently, Director, Office of Human Resources Management, FEMA)

The following individuals attended and participated in Board meetings:

Patricia M. Gormley

General Counsel, FEMA

Jerry E. Johnson

Management Analyst, Staff Planning & Evaluation
Office of Administrative Support, FEMA

Franklin E. Kameny

Personnel Security Paralegal, Gay Rights Activist

David A. Ross

Office of General Counsel, FEMA

Office of Management Services (Consultant to the Board), FEMA

Mary E. Weindorf

Secretary, Office of Management Services, FEMA



Federal Emergency Management Agency

Washington, D.C. 20472

JUL 31 1992

MEMORANDUM FOR: All FEMA Employees

FROM: ^{RGT} LTG Richard G. Trefry (USA-Ret.)
Chairman, Security Practices Review Board

SUBJECT: Invitation to Comment to the Board

The FEMA Security Practices Review Board is currently conducting a review of security practices, processes and procedures within FEMA. The Board operates under the provisions of the Federal Advisory Committee Act and, quite simply, is attempting to:

- Review the practices and processes involved in the FEMA Security Program,
- Provide recommendations to appropriate authorities to improve the FEMA Security Program.

During the July 24, 1992, meeting of the Board at FEMA, the Board considered and recommended that employees of FEMA should be given the opportunity to provide any observations or comments concerning current FEMA security practices.

Accordingly, this memorandum invites any FEMA employee to provide the Board with any observations, recommendations, comments, etc., concerning this matter, subject to the following:

- All comments should address the policies and procedures involved in the generic matter of security. The Board is neither empowered to nor physically capable of addressing individual security problems or complaints in this broad area.

- Comments must be in writing and preferably should be signed by the person submitting the observation. Anonymous submissions are not encouraged. A sincere and conscientious effort will be made by the Board to protect the confidentiality of any person submitting comments. Individuals desiring to comment should forward their comments in writing to:

LTG Richard G. Trefry (USA-Ret.)
Chairman, Security Practices Review Board
2425 Wilson Boulevard, Room 670
Arlington, VA 22201

The Board will consider and appreciate any efforts concerning this invitation by the employees of FEMA in this important matter.

Tab D

**AN ANALYSIS OF
THE PERSONNEL SECURITY PROCESS**

TAB D - THE PERSONNEL SECURITY PROCESS

The Board devised a series of charts to clarify and explain the process and procedures in the FEMA personnel security program.

Enclosure 1 (Position Risk . . . System)

Enclosure 1 to Tab D describes the new risk/sensitivity level designation system that was established in 1991 by the Office of Personnel Management (OPM). This new system is described in Chapters 731 and 732 of the Federal Personnel Manual (FPM), an official OPM publication.¹

OPM also requires the head of each agency to designate risk levels for every competitive service position in accordance with certain uniform criteria in Chapter 731. The head of each agency is also required to designate sensitivity levels for national security positions in accordance with Executive Order 10450. Chapters 731 and 732 provide guidelines for these separate designations.

It must be understood that FPM Chapters 731 and 732 describe separate designation requirements. As a result, a "public trust" position would not, by itself, require a security clearance. However, what is generally not understood is that a "public trust" position, which can be designated as either moderate or high risk under Chapter 731, can require an investigation that is comparable in time and expense to that required for a national security position under Chapter 732 (Enc. 2).²

While OPM was establishing its new risk/sensitivity level system, as outlined in Enclosure 1, FEMA was still in the process of establishing a "position sensitivity" program as required by the previous (pre-1991) OPM position designation system. The absence of such a program at FEMA had

¹ See Page D-13.

² See Page D-13.

been noted by OPM in its March 1989 appraisal report. The Board was informed that FEMA had already taken steps to correct this problem but had not yet established its position sensitivity program before OPM had completed its appraisal. FEMA may now have to modify whatever sensitivity program it has established in order to incorporate the new risk/sensitivity system. In view of the recent changes to the position designation system, the Board recommends that a FEMA senior executive carefully and continually review all positions, especially those designated as "public trust" or national security. This review will ensure that they are assigned the appropriate risk and/or sensitivity levels in accordance with the new risk and sensitivity level designation system and FEMA requirements for security clearances.

As stated previously, there is a culture existing in FEMA that a security clearance is required for social status, as well as for promotion. The Board believes that this is pernicious and must be eliminated. However, any removal of clearances must be accomplished in a nonprejudicial manner. This is an absolute requirement. The Board further recommends that FEMA develop and conduct a program to educate its employees on the revised security clearance policies and explain in detail the reasons for the reductions in the number of clearances.

A review of the FEMA mission statement by the Board disclosed no express requirement for any classified activity. However, in fact, a number of elements of the mission do require security protection and access to classified information. The Board therefore recommends that FEMA modify its mission statement to include this requirement. The Board also recommends that FEMA management review its "organization and functions" manual and any personnel security regulations to ensure that they are consistent and accurately describe all personnel security requirements and assignments.

The Board believes that personnel security problems will not disappear until appropriate training is provided to all levels of management concerning risk and/or sensitivity level designations, security clearances, and the evaluation/determination process.

Enclosure 2 (Types/Scope/Costs of Investigations)

The Board was particularly interested in the differences in scope (years) among the four types of background investigations that are or will be used at FEMA. They are:

- National Agency Check with Inquiries (NACI)
- Limited Background Investigation (LBI)
- Background Investigation (BI)
- Single Scope Background Investigation (SSBI)

Enclosure 2 illustrates the primary differences between the types, scope and costs of background investigations.³

Enclosures 3-8 (The FEMA Hiring/Clearance Process)

Enclosures 3-8 are sequential flow charts that summarize the hiring/security clearance process at FEMA. There are five basic steps:

1. Requirements Established (Enc. 3)
2. Application (Enc. 4)
3. Investigation (Enc. 5)
4. Evaluation and Adjudication
 - a. Suitability (Enc. 6)
 - b. Security Clearance (Enc. 7)
5. Determinations/Appeals (Enc. 8)

Enclosure 3 (Requirements)

Enclosure 3 depicts the initial step in the FEMA hiring/security clearance process. It depends on the existence or establishment of a risk and/or sensitivity level for each position (Enc. 1). The appropriate program manager then submits a Standard Form (SF) 52 to the Office of Human Resources Management (HRM). The risk and/or sensitivity level is mentioned in the SF 52. This submission is supported by a position

³ See Page D-14.

description and an Optional Form 8, which requires official certifications concerning the position description and the classification/grade of the job.

Upon validation by HRM, a vacancy announcement is made, inviting applicants to apply for the position. The position announcement also identifies the designated risk and/or sensitivity level.

The Board was unable to determine exactly who in FEMA reviews the SF 52 and the position description to ensure that the risk and/or sensitivity level designation is appropriate. The Board recommends that FEMA prepare an internal guidance document to ensure that its risk and sensitivity level criteria and security clearance requirements are described and implemented correctly.

Enclosure 4 (Application)

Enclosure 4 illustrates the various actions taken within FEMA when a person applies for a vacant position.⁴

Enclosure 5 (Investigation)

Enclosure 5 describes the background investigation process on the basis of the particular questionnaire completed by the job applicant. The Board determined that HRM initiates the National Agency Check with Inquiries (NACI) for only nonsensitive (low risk) positions. It normally requires from three to six months to complete a NACI. For "public trust" and national security positions, the Office of Security (SY) initiates the appropriate investigation (LBI, BI, or SSBI). The NACI, LBI, BI, and SSBI are conducted for FEMA by OPM.

⁴ See Page D-14.

The Board was concerned that FEMA appears to grant a large number of waivers of pre-appointment investigations.⁵ These waivers appear to be the result of the length of time required to complete the investigative/adjudicative process under normal procedures. They also appear to be granted because of a perception by FEMA management that there is an "immediate need" to fill a position. The waiver authority, however, derives from Executive Order 10450, which permits waivers only in cases of a bona fide "emergency" (Tab E, Enc. 6). The Board believes that the culture mentioned previously, which requires everyone to either occupy a position of "public trust" or have a security clearance, aggravates and contributes to the large number of waivers requested and apparently required. There is the further problem of wanting to hire quality applicants who do not have clearances and are often not willing to stand in line waiting for an appointment while the inexorable background process grinds away.

The Board also found that it could not determine from the OPM regulations or the FPM whether or not a waiver from a pre-appointment investigation (LBI, BI) is permitted for a "public trust" position. The Board recommends that FEMA bring this issue to the attention of appropriate authorities for resolution.

Enclosure 6 (Suitability Evaluation and Adjudication)

Enclosure 6 describes the process of evaluating and adjudicating an application for any position. It also identifies the eight potential "suitability" disqualifiers established by an OPM regulation (Tab E, Enc. 8).

The Board ascertained that a recent FEMA Instruction delegated responsibility for the making of suitability determinations to the Director, HRM, for nonsensitive (low risk) and "public trust" positions and to the Director, Office of Security, and the Chief, Personnel Security Division, for only sensitive or national security positions. The Board also determined by interrogation that a determination of unsuitability is

⁵ See Page D-14.

generally coordinated with HRM, the immediate supervisor of the job applicant, and Office of Security personnel.

The Board believes that the current delegation of responsibilities for suitability determinations requires clarification. The Board therefore recommends that FEMA modify its recent delegation of suitability determination authority so that HRM would have sole responsibility for making all basic, i.e., Part 731, suitability determinations (Enc. 6) for all positions. This change would allow the Office of Security to focus on and make determinations having only national security implications, such as the granting of security clearances (Enc. 7).

Enclosure 7 (Clearance Evaluation and Adjudication)

Enclosure 7 isolates the security clearance determination functions of the Office of Security. It also lists the potential disqualifying security risk and loyalty criteria from Executive Order 10450 that are used to evaluate applicants and employees for a clearance or any national security position that does not require a clearance. The Board observed that at least five (*) of these disqualifiers have a similar counterpart in the suitability disqualifiers listed in Enclosure 6.

Similar observations were made in 1957 by the Commission on Government Security (Wright Commission) in its report to the President and Congress. In addressing the consequences of EO 10450, which merged basic suitability factors with security risk and loyalty factors (Tab E, Enc. 6), it made certain recommendations for clarifying the personnel security program. These recommendations were supported by the following observations at page 44 of its report:

. . . while the current [personnel security] program has been labeled and justified as a security program, it has in practice been an unnatural blend of suitability, loyalty, and security programs. The hybrid product has been neither fish nor fowl, resulting in inconclusive adjudications, bewildered security personnel, employee fear and unrest, and general public criticism.

The Board finds that these observations still have merit and deserve further review.

Enclosure 8 (Suitability/Clearance Determinations/Appeals)

Enclosure 8 summarizes the final phase of the hiring/clearance process at FEMA. This phase applies to both conditional hires, who are allowed to begin work on the basis of a waiver of the preappointment investigation, and tentative selectees, who are not allowed to begin work before the completion of the investigation and adjudication process.

Enclosure 8 also identifies certain administrative and judicial organizations outside of FEMA, such as the Merit Systems Protection Board (MSPB) and the Court of Appeals for the Federal Circuit. These organizations may be available to a FEMA job applicant who has been tentatively selected for a position or conditionally hired on the basis of a waiver but has failed to overcome certain suitability or clearance disqualifiers after the completion of the necessary background investigation and adjudication process. The Board has been advised that the availability of an appeal to these bodies is subject to various "jurisdictional" requirements that can often preclude any review of a case, especially on the merits of an agency action. The Board has also been advised that this appeal process, however limited, may be even more difficult and limited for probationary employees or applicants who are denied or lose a job because of failure to meet security clearance requirements (Enc. 7).⁶ In any case, on the basis of information made available to the Board, the distinct appellate processes identified in the chart are those required or allowed by legal authorities and followed by FEMA.

Given the limited appellate process with respect to unfavorable security clearance actions, the Board recommends that the Director of FEMA continue to have ultimate responsibility for making all final determinations involving the denial, suspension or revocation of security clearances.

⁶ See Page D-14.

Enclosures 9-11 (Post-Employment Determinations . . . Appeals)

Enclosures 9 and 11 depict the post-employment investigation and determination process that can confront a FEMA employee. This process can be triggered by a derogatory allegation from within or without the Agency (Enc. 9). An investigation will also result from periodic reinvestigation requirements for "public trust" and national security positions (Enc. 10). An opportunity for promotion, reassignment, or change of duties to a higher risk and/or more sensitive position may also require a new or updated investigation and determination (Enc. 11).

In the case of periodic reinvestigations, the Board determined that they are sometimes postponed because of the lack of funds. Since these kinds of delays, for whatever reason, can have serious consequences to sensitive missions at FEMA, the Board recommends that FEMA management take immediate action to correct this problem and bring it to the attention of the highest security authorities within the Administration and Congress.

In cases where the individual is already a FEMA employee and an investigation leads to a determination of unsuitability, and/or the suspension or revocation of a security clearance, the Board considered it appropriate to provide in-house legal assistance to these individuals. The Board was informed that in the course of a year about 30 such adverse determinations are made. The Board also believes that not all of the affected persons would require legal assistance, nor find it desirable; rather, such assistance would be an available option.

Enclosure 12 (Summary of . . . Determination Process for a Moderate Risk Public Trust Position)

Enclosure 12 is a flowchart that summarizes the process described in Enclosures 1-6 and 8-10 for one selected position, a moderate risk "public-trust" position. This position falls between a nonsensitive/low risk position and a high risk "public trust" or critical sensitive/special sensitive (national security) position.

According to FPM Chapter 731, a "public trust" position has the potential to adversely affect the integrity, efficiency, or effectiveness of assigned government activities. For example, positions having the authority to commit government funds through grants, loans, or contracts are considered to be "public trust" positions. A significant number of operational positions in FEMA, especially those in disaster assistance activities, could come under this position category.

A "moderate risk public trust" position has the potential for only "moderate to serious impact" on the efficiency of the service. In contrast, a "high risk public trust" position would have an "exceptionally serious impact."⁷

After OPM completes its investigation, it submits the Report of Investigation (ROI) to the Office of Security (SY) (Enc. 5). The ROI is then submitted by SY to HRM to make the appropriate determination (Encs. 6,8).

⁷ See Page D-15.

GENERAL COMMENTS

The Board recommends that the terminology used to describe the various steps in the personnel security process be clarified. The Board found the following terms more understandable than some of the terms currently in use:

- a. Requirement
- b. Application
- c. Initiation
- d. Investigation
- e. Evaluation
- f. Recommendation
- g. Determination

The Board considers the term "adjudication" to be especially ambiguous and misleading. (As a matter of interest, adjudication in the FEMA Office of Security is accomplished by contract personnel.) The Board is also concerned that the description of functions under the present system is easily misinterpreted. This has led to an understandable perception that the Office of Security, as the investigator, the evaluator, the adjudicator, and the decisionmaker, is an entity accountable only to itself and the personnel security system. This arrangement might best be described as making one organization act as the sole "investigator, prosecutor, judge and jury."

The Board recommends that FEMA management specifically assign responsibility for each step (a through g) in the personnel security process to either management or staff, with the Office of Security only providing staff recommendations to FEMA management in these important matters, and the Director, FEMA, making all final decisions, i.e., all final appeal determinations. The present system is not fair to the Office of Security, its Personnel Security Division, management, or to FEMA as a whole. It is easy to understand why the perception exists, and is frequently reinforced, that only the Office of Security is "in charge" of every step of the personnel security process.

As stated previously, the Board is convinced that the number of security clearances in FEMA is excessive. On the basis of sensitive operational requirements that involve FEMA employees and programs, the need for security clearances is extremely limited. Instead, the need for security clearances is largely based on the exposure of FEMA employees to ° classified information. The Board believes there are administrative and operational techniques to cope with this problem and reduce the need for so many clearances. As stated earlier, the Board recommends that the number of security clearances be sharply reduced and believes that a goal of approximately 300 security clearances within FEMA would not be unrealistic.

The Board has also noted that FEMA management needs to initiate a comprehensive analysis of security clearance requirements in order to validate and determine the need for these and other reductions. This analysis will undoubtedly lead to further reductions that would still allow FEMA to perform its missions effectively. This would include adoption of accurate classification guides for all FEMA programs, functions, and activities.

Finally, the Board recommends that FEMA use the contents of Tab D as the basis for detailed and explicit instructions on the personnel security system and practices within FEMA.

END NOTES

1. FPM Chapters 731 and 732 are OPM guidelines that implement the OPM regulations included in Tab E, Enc. 8. Enclosure 1 is based on the "Position Designation Matrix" in Appendix A to FPM Chapter 731. Chapter 731 also describes a basic "suitability" program for nonsensitive (low risk), "public trust," and computer/ADP positions. Chapter 732 establishes various guidelines on the implementation of Executive Order 10450 (Tab E, Enc. 6) for "national security positions" by describing certain "sensitivity" level criteria and the appropriate investigative requirements.

Suitability, for purposes of Chapter 731, is defined in terms of "effectiveness and efficiency" in performing a particular job as measured by certain identifiable character traits and prior conduct (Enc. 6). A national security position, for purposes of Chapter 732, is defined in terms of certain activities that basically concern the protection of the United States from foreign aggression or espionage or requirements for access to classified information (Tab E, Enc. 8).

2. This outcome can result from the OPM scoring or "point" system, which, as indicated by the dotted lines in the chart, can require consideration of both risk and sensitivity level scores in order to determine the type and scope of the background investigation needed for a particular position (Enc. 2). For example, a person being considered for appointment to a "high risk" computer/ADP position with "noncritical sensitive" national security duties, but without access to classified information, would, if hired, be required to complete the more comprehensive SF 86 (on account of national security duties) rather than the less intrusive SF 85P. In addition, because of the "high risk" designation, a 5-year Background Investigation (BI) would be required. A "moderate risk" designation, however, would have required only a 3-year Limited Background Investigation (LBI). Additional information on "public trust" positions, in general, and a moderate risk position, in particular, is included in the description of Enclosure 12. (It should also be noted that some of the items in the SF 86 would require information for the last

15 years while the scope of the actual field investigation would only cover the past 5 years (Enc. 2).)

3. The SSBI is a new 10-year background investigation established by President Bush in 1991 through National Security Directive 63. It replaces the 15-year Special Background Investigation (SBI) and the BI for national security positions. The BI will still be used, however, for high risk "public trust" positions. In addition, the scope of the BI and LBI has also been reduced from 7 to 5 years and from 5 to 3 years, respectively. The NACI, however, will still cover 5 years.

4. The SF 171 is the basic application form used by the Federal Government to establish the qualifications of the applicant for the position. Additional forms, such as the SF 85, are used to initiate background investigations once an applicant is either tentatively selected but not yet hired or conditionally hired and allowed to start work on the basis of a waiver from a pre-appointment background investigation (Enc. 5).

5. The effect of the waiver from the preappointment investigation is to allow an applicant who has been tentatively selected for a certain position to start work with the Agency before the required investigation process is completed. Without a waiver, a person tentatively selected for a certain position must await the completion and favorable outcome of the investigation process before he can start work at the Agency (Encs. 6,8). Enclosure 5 basically covers only these two situations. Thus, it may not cover persons who are hired on a one-year probationary basis or who are hired subject to a suitability investigation, which, with certain exceptions, expires automatically after one year (Tab E, Enc. 8).

6. These difficulties and limitations are the result of a 1988 United States Supreme Court case, Department of the Navy v. Egan, which allowed the MSPB to avoid or preclude review of security clearance denial actions on the merits (Tab E, Enc. 5). Thus, as the chart indicates, any challenge on the merits to the denial or revocation of a security clearance can probably be appealed no further than the head of an agency. This absence of any right to appeal to a higher authority outside the Agency is also supported by and consistent with the provisions of EO 10450 and its

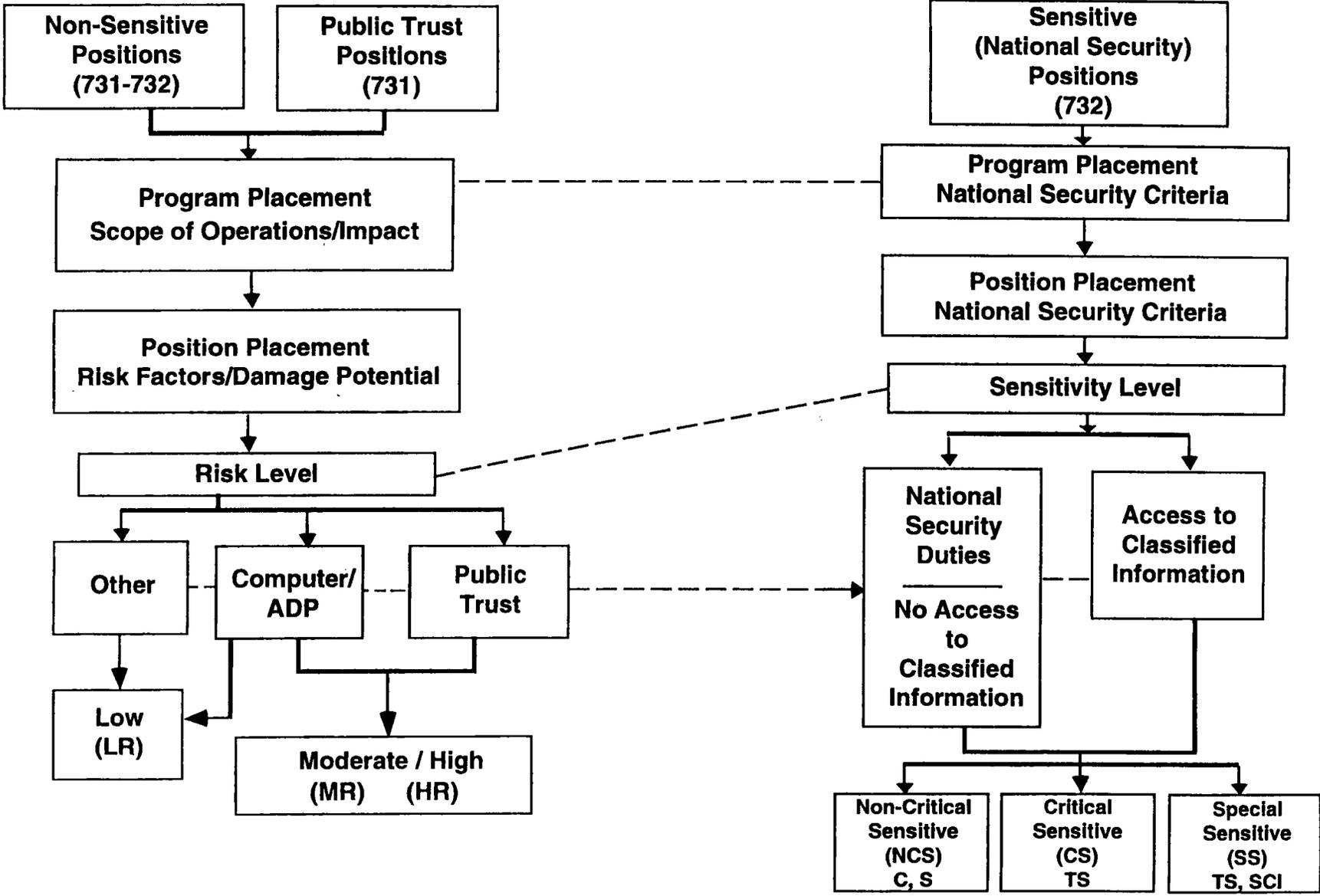
authorizing legislation (Tab E, Encs. 5-6). The Board has not attempted to address any other legal remedies based on Constitutional claims that may be available to persons denied security clearances, but understands another 1988 Supreme Court case, Webster v. Doe (486 U.S. 592), may allow such claims to be pursued in the Federal courts.

7. The appropriate risk level designation depends on a scoring system described in Appendix A to FPM Chapter 731 (Enc. 1). Enclosure 12 describes a position that would fall into one of nine possible risk level categories, depending on the "impact" of the given program on agency operations, i.e., major, substantial, moderate, or limited. For example, a position with "substantial impact" and position risk points from 11-29 would qualify for a "moderate risk" designation. If this position scored in the higher range, i.e., 18-29 points, it would require a Limited Background Investigation (LBI).

The current LBI has a three-year scope (Enc. 2) and relies initially on the SF 85P completed by the tentative selectee (Enc. 4). The actual LBI is conducted through the Office of Personnel Management (OPM) and includes a National Agency Check (NAC), which provides access to National Criminal Information Center (NCIC) records maintained by the FBI, and certain other actions, such as a subject interview to verify information and/or clarify discrepancies on the SF 85P and independent verifications through a field investigation.

The SF 85P requires answers to 21 separate questions while the SF 85 (nonsensitive/low risk position) only requires answers to 11 questions. The additional questions on the SF 85P cover a variety of topics, including the subject's relatives, investigations record, outside activities, police, financial and medical records, and foreign countries visited by the subject. The scope of most of these additional questions range from 5 to 10 years. There is no time limit on the scope of the investigation and medical records questions.

Position Risk/Sensitivity Level Designation System



Types/Scope/Costs of Personnel Security Investigations and Questionnaires Based on Risk/Sensitivity Levels

TYPE & SCOPE (YEARS) OF INVESTIGATION	NACI (5)	LBI (3)		BI (5)	SSBI (10)
POSITION	NON-SENSITIVE	PUBLIC TRUST	NATIONAL SECURITY	PUBLIC TRUST	NATIONAL SECURITY
FPM CHAPTER	731	731	732	731	732
TYPE & SCOPE (YEARS) OF QUESTIONNAIRE	SF 85 (1-5)	SF 85P (5-10)	SF 86 (5-15)	SF 85P (5-10)	SF 86 (5-15)
RISK LEVEL	LR	MR	MR	HR	HR
SENSITIVITY LEVEL	NS	—	NCS	—	CS, SS
<u>OPM BILLING RATES</u> TIME	<u>\$50</u> 75 DAYS	<u>\$1850 - 1400</u> 35-120 DAYS		<u>\$2850 - 2400</u> 35-120 DAYS	<u>\$3150 - 2700</u> 35-120 DAYS
<u>FEMA ACTUAL COSTS</u> TIME	<u>\$50</u> 120 DAYS	<u>\$1850</u> 60-120 DAYS		<u>\$2850</u> 60-120 DAYS	<u>\$3150</u> 60-120 DAYS

Hiring / Clearance Process

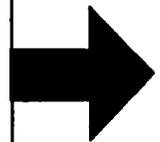
1. Requirement Established

Program Manager submits to Human Resources Management (HRM):

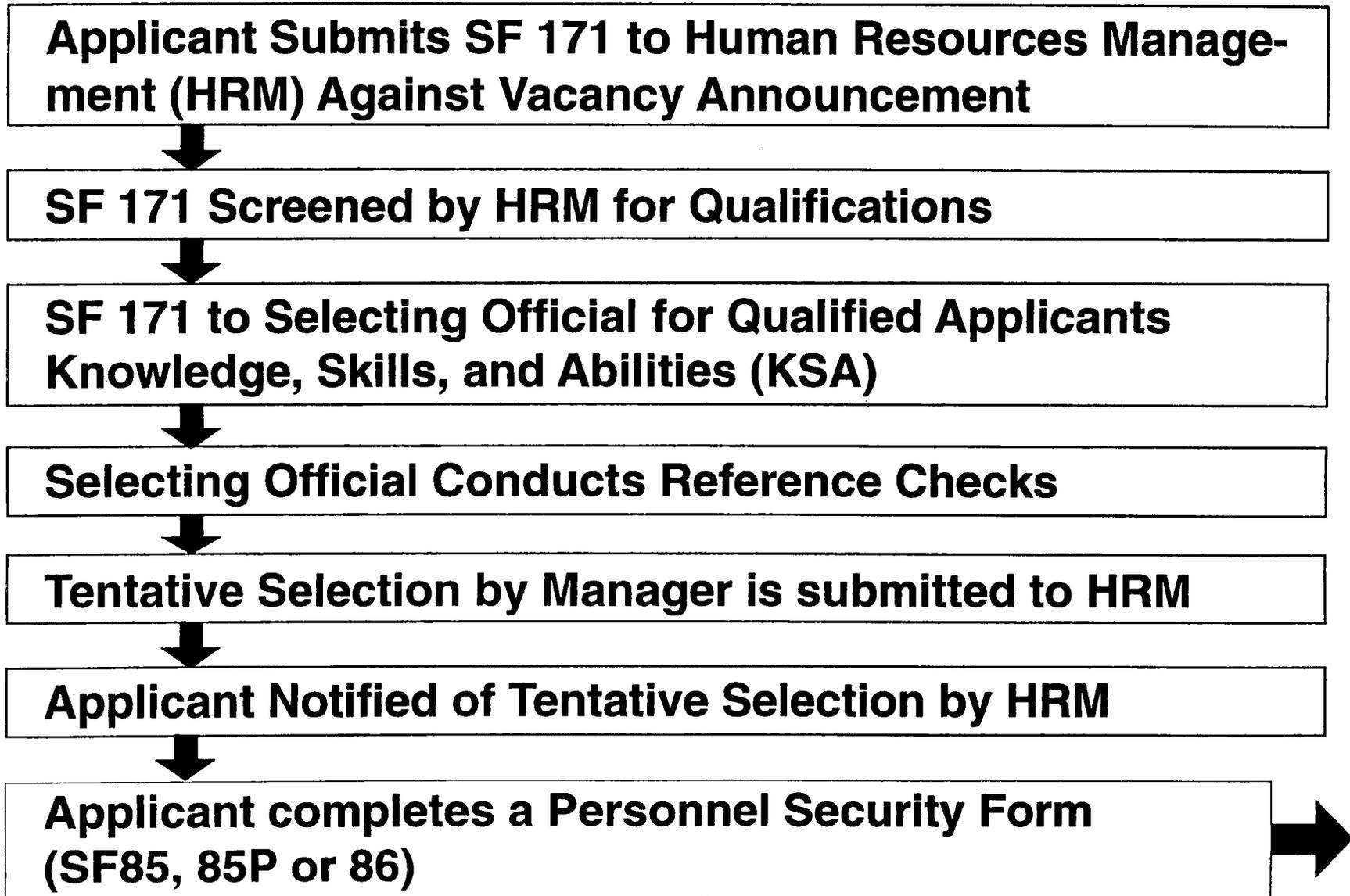
- **Standard Form (SF) 52 (Includes Risk and/or Sensitivity Level)**
- **Position Description**
- **Optional Form 8**



**Vacancy Announcement by HRM
(Includes Risk and/or Sensitivity Levels)**



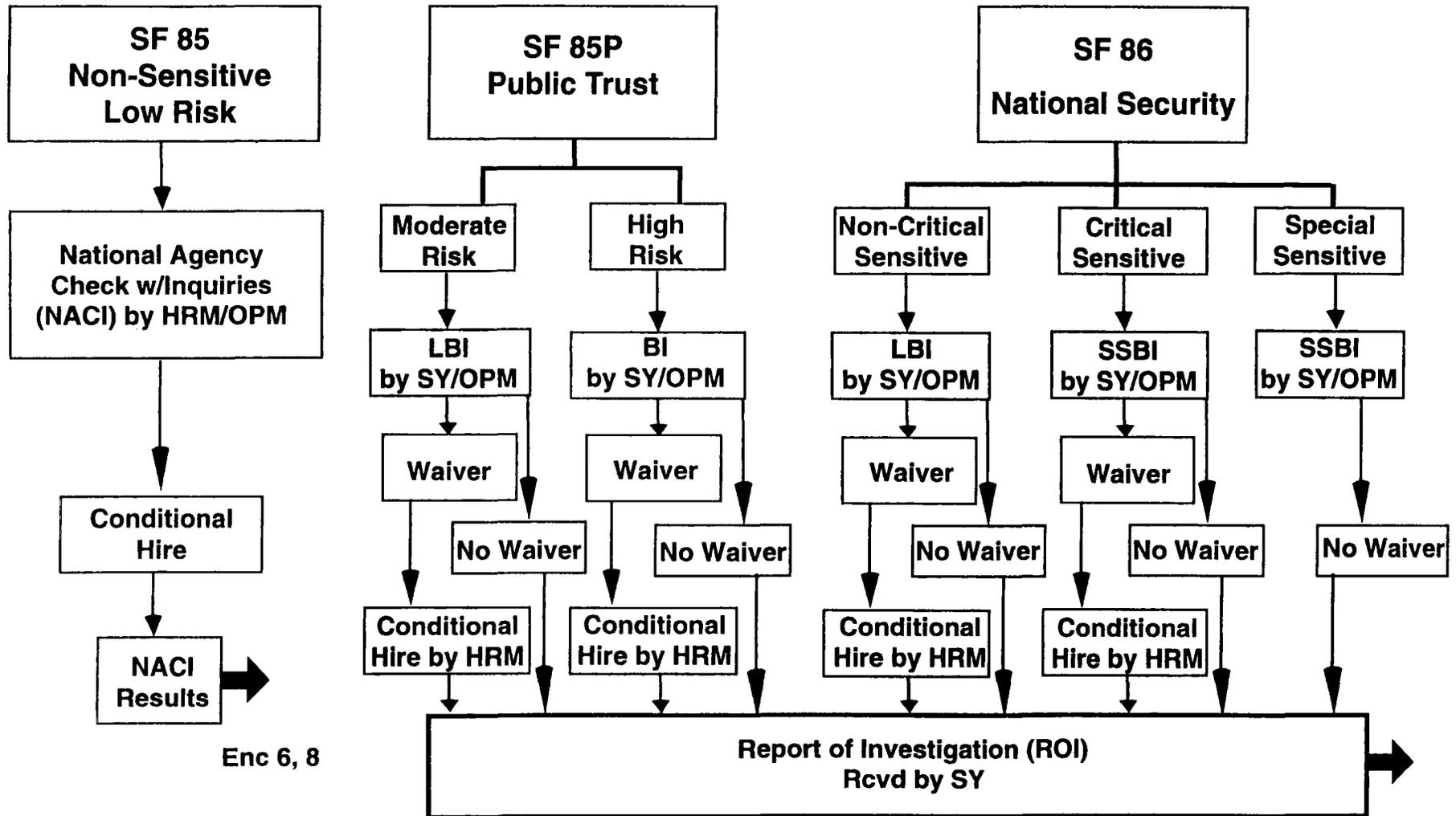
2. Application



3. Investigation

Investigation Initiated by Human Resources Management (HRM) /Security (SY)

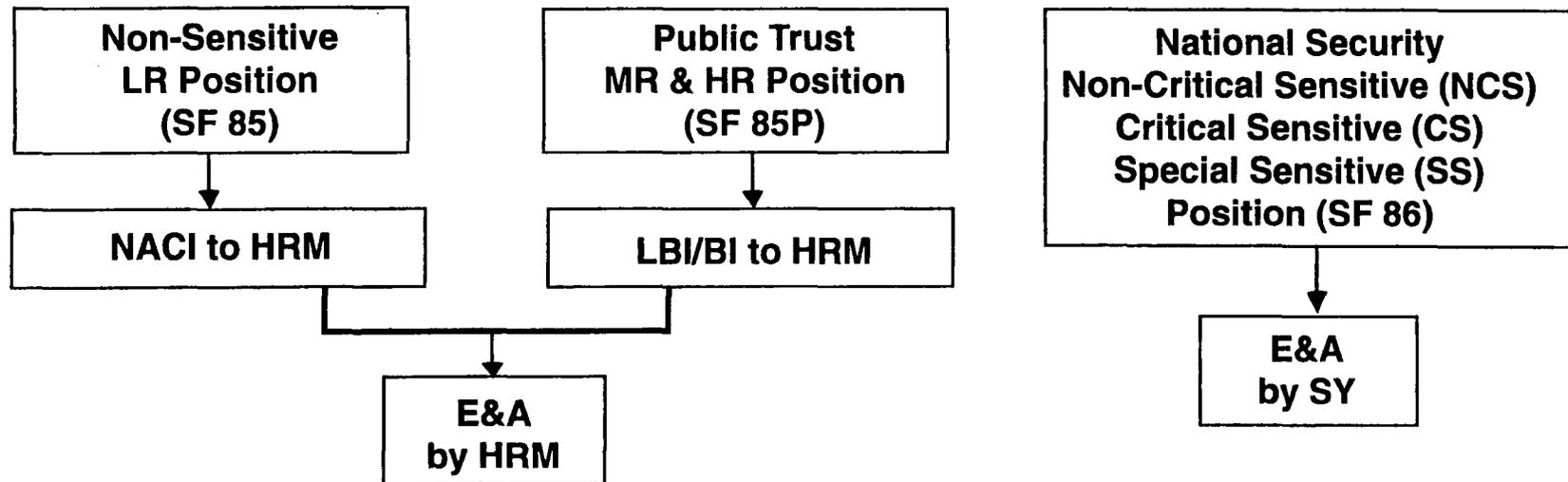
Based on Risk/Sensitivity Level



Enc 6, 8

Enc 6-8

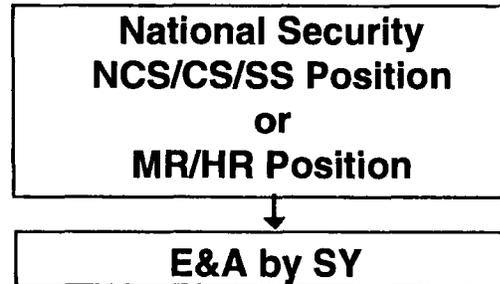
4a. Suitability Evaluation & Adjudication (E&A)



SUITABILITY DISQUALIFIERS from Title 5, Code of Federal Regulations, Part 731

1. **Misconduct / Negligence**
2. **Criminal / Dishonest Conduct**
3. **False Statement**
4. **Refusal to Furnish Required Testimony**
5. **Alcohol Abuse**
6. **Illegal Drug Use**
7. **Acts Designed to Overthrow U.S. Gov't**
8. **Statutory Bar (OPM)**

4b. Clearance Evaluation & Adjudication

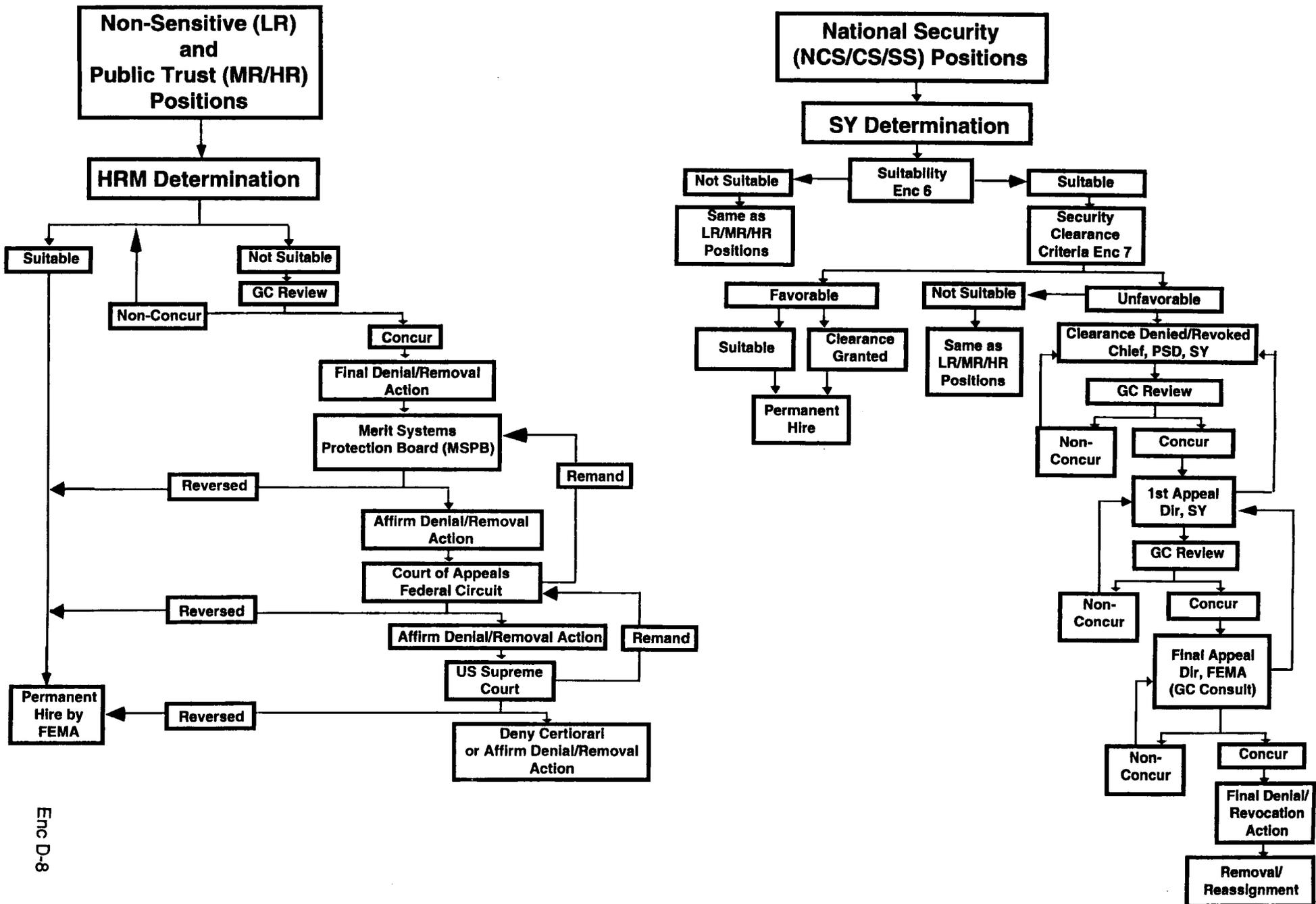


DISQUALIFYING SECURITY CRITERIA (EO 10450)

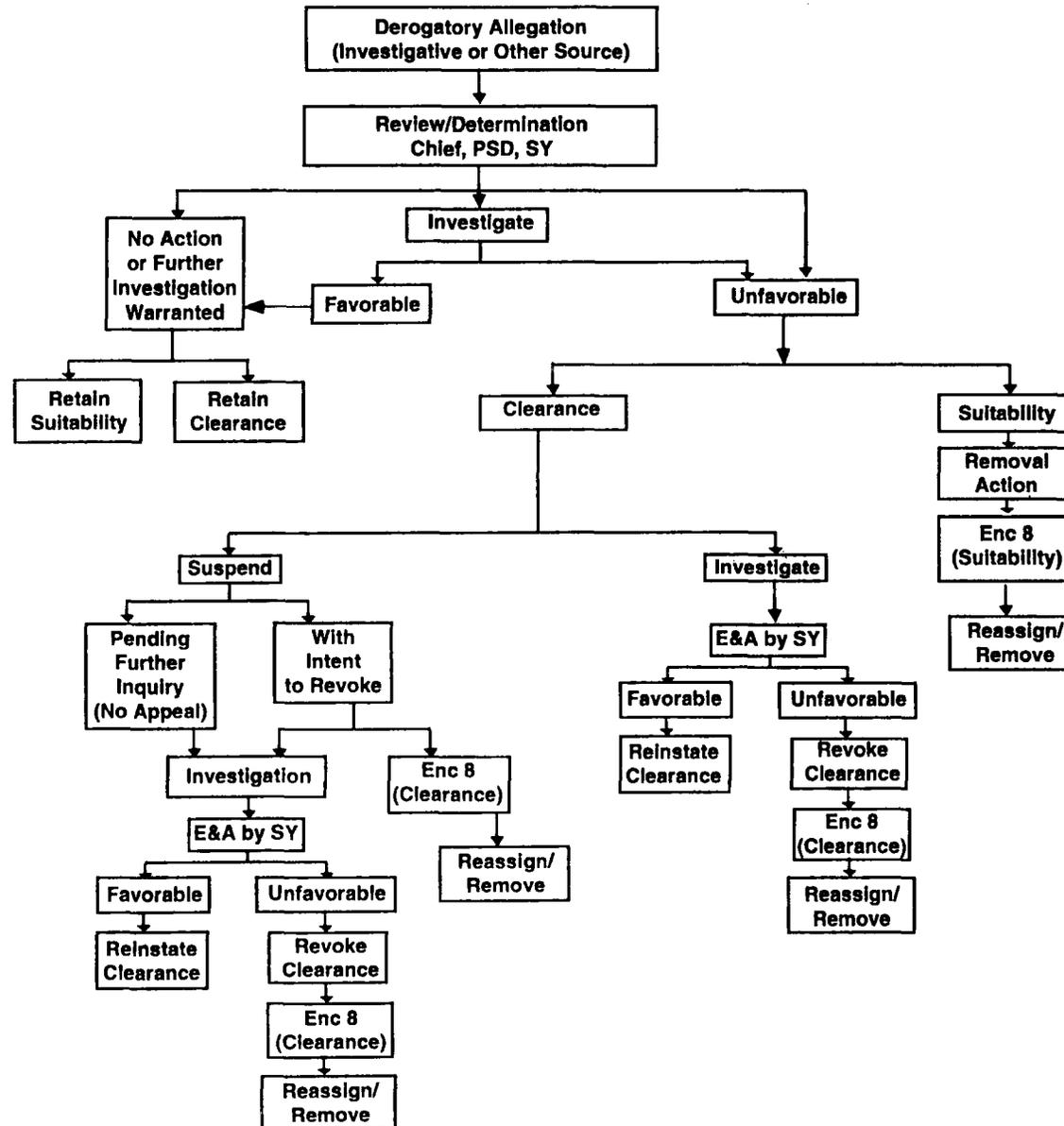
1. Not Reliable / Trustworthy
- * 2. Falsification
- * 3. Criminal / Dishonest Conduct
 - * Illegal Drug Use
 - * Alcohol Abuse
4. Illness / Mental Condition
5. Coercion / Influence
- * 6. Sabotage, Espionage
7. Advocate Overthrow of U.S. Gov't
8. Association with Saboteur, Traitor
9. Membership in Organization to Prevent Exercise of Rights Under Constitution or Overthrow U.S. Gov't
10. Disclosure of Security Info Where Prohibited
11. Serve Interest of Another Gov't in Preference to U.S.
12. Refusal to Testify

NOTE: Each criteria with an asterisk (*) has a counterpart in the Suitability Disqualifiers listed in Enclosure 6.

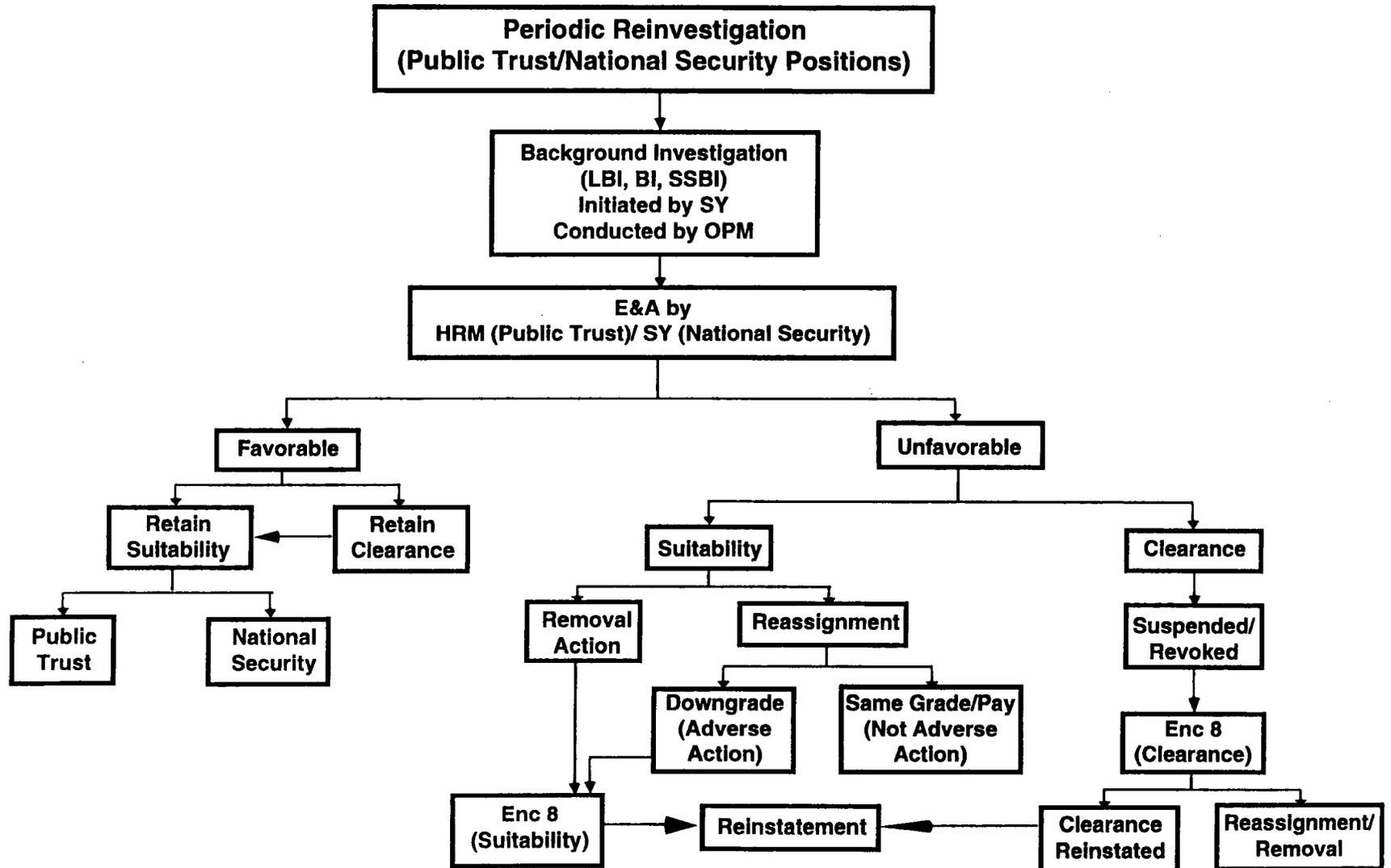
5. Suitability and Clearance Determinations/Appeals



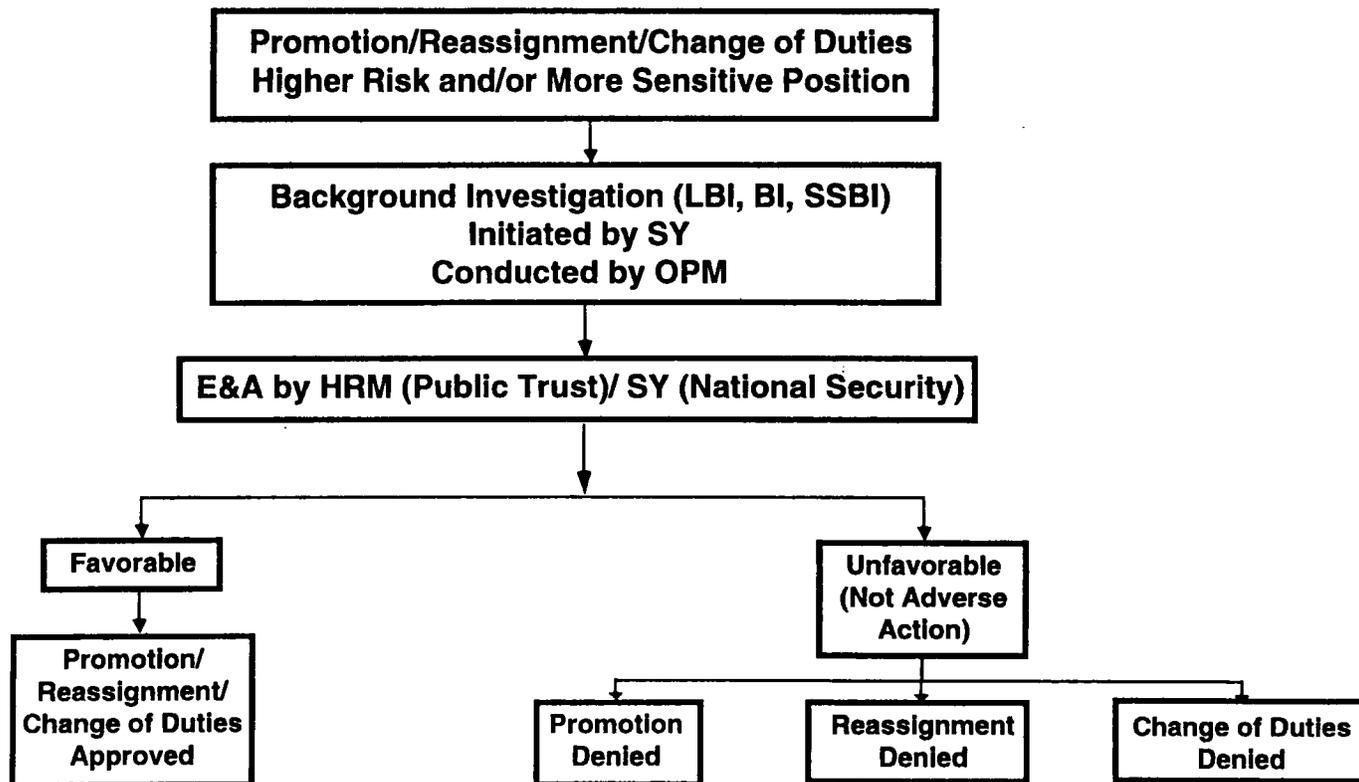
Post-Employment Investigations/Determinations/Appeals (Based on Derogatory Allegation)



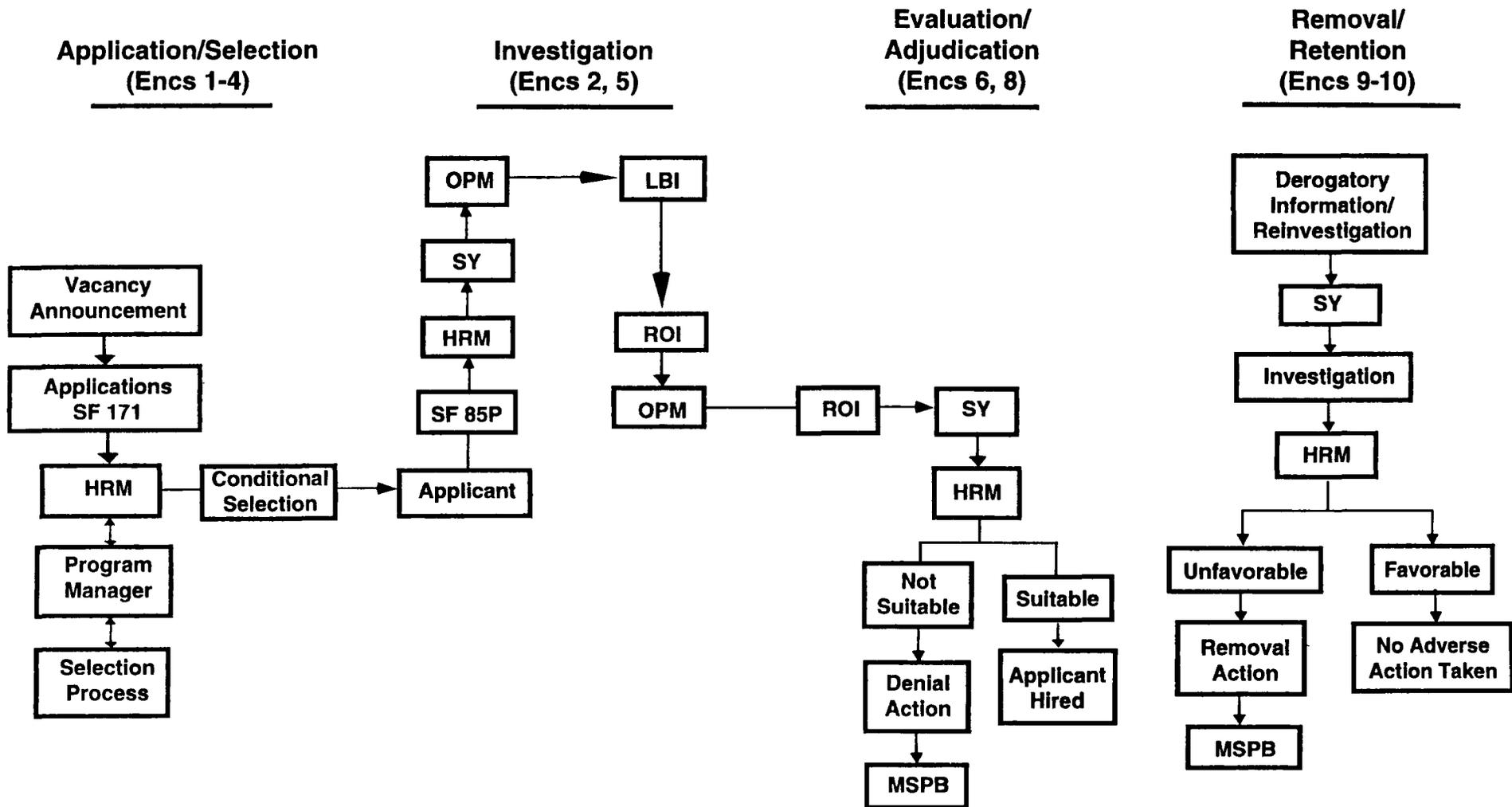
Post-Employment Investigations/Determinations/Appeals (Periodic Reinvestigation)



Post-Employment Investigations/Determinations/Appeals (Promotion/Reassignment)



Summary of Pre- and Post-Employment Determination Process for a Moderate-Risk Public Trust Position



PERSONNEL SECURITY AUTHORITIES

Introduction

Enclosures 1-8 to Tab E contain charts, matrices, and other descriptive and explanatory information on existing personnel security authorities applicable to the President and federal departments and agencies. Further information on the footnotes and other symbols used in the charts and matrices is contained in the notes below.

Enclosures

Subjects

- | | |
|---|---|
| 1 | "Schematic for Executive Order 10450/5 CFR Part 732 Authorities" (Sensitive or National Security Positions). |
| 2 | "Schematic for Executive Order 12356" (Security Classifications and Clearances). |
| 3 | Matrix on "Rule Making Authorities relied upon by OPM to promulgate 5 CFR Parts 731, 732, 736" (old and new). |
| 4 | Footnotes to Enclosures 1, 2, and 3. |
| 5 | "Synopsis of Personnel Security Authorities." |
| 6 | Executive Order 10450. |
| 7 | Executive Order 12356. |
| 8 | 5 CFR Parts 731, 732, 736 (OPM's new Interim Final Regulations). |

For additional information on Enclosures 1-5, see "Notes" on the following page.

Notes:

Enc. 1. A copy of "Executive Order 10450," which was issued by President Eisenhower in 1953, is at Enc. 6. The reference to "5 CFR Part 732" is to a new personnel security regulation of the Office of Personnel Management (OPM) that is codified in Title 5, Code of Federal Regulations (CFR), Part 732. A copy of this new regulation is at Enc. 8. The numbered paragraph (¶) references in Enc. 1 are found in Enc. 5. The numbered footnote references appearing after the United States Code (USC) and Executive Order (EO) 10450 citations are listed and summarized in Enc. 4.

Enc. 2. A copy of EO 12356, which was issued by President Reagan in 1982, is at Enc. 7. The numbered paragraph (¶) references in Enc. 2 are found in Enc. 5.

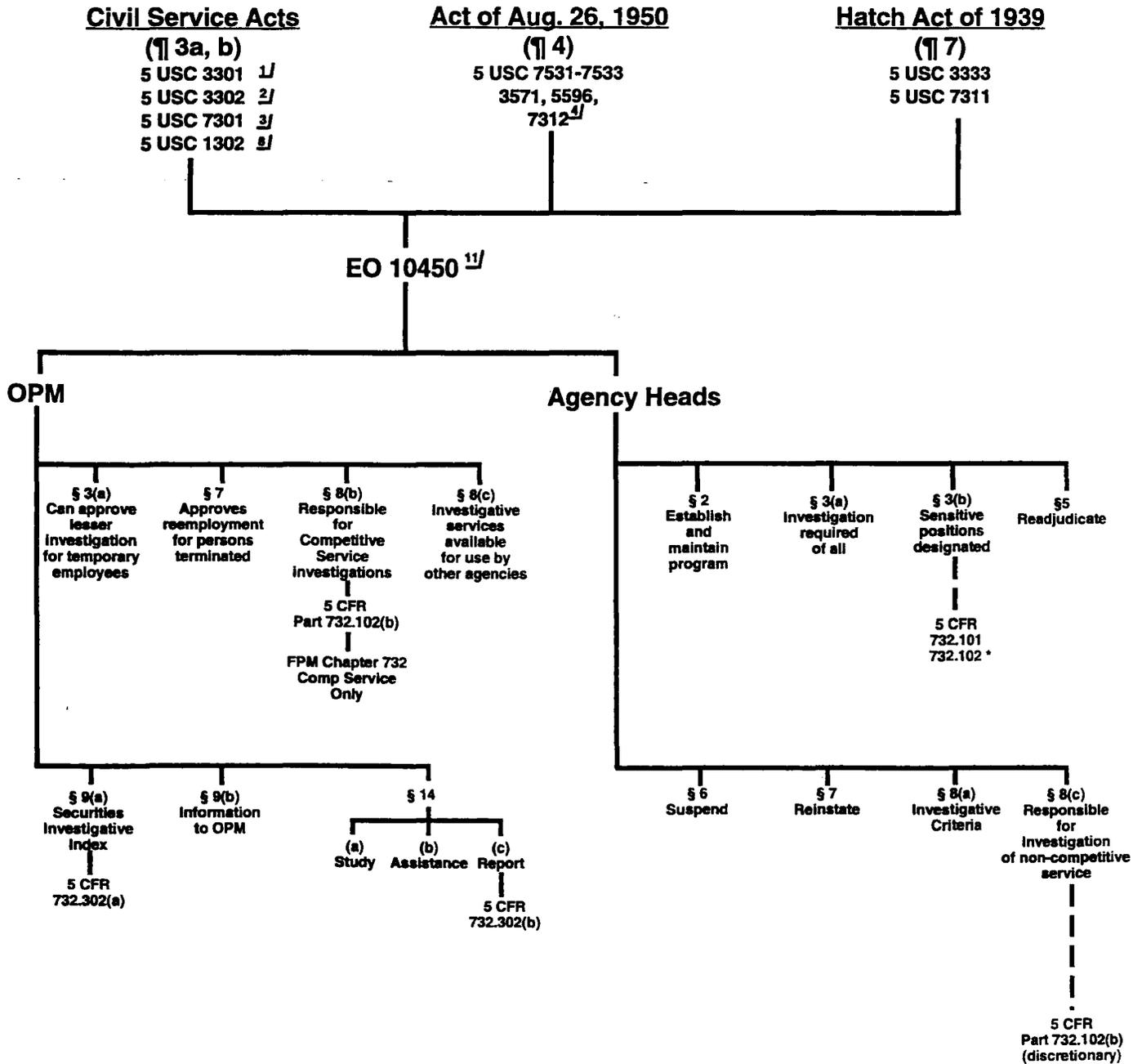
Enc. 3. Copies of the new OPM regulations are provided in Enc. 8. The numbered footnote references in Enc. 3 appearing after the USC and EO citations are listed and summarized in Enc. 4.

Enc. 4. The numbered paragraph (¶) references in Enc. 4 are found in Enc. 5. The numbered footnotes appearing after the EO and USC references are to the footnotes in Enc. 4.

Enc. 5. The "synopsis" does not reflect the revocation of EO 11222 (¶ 13) by EO 12674 of April 12, 1989, "Principles of Ethical Conduct for Government Officers and Employees," which is codified at page 215 of the 1989 compilation of Presidential Documents in Title 3 of the Code of Federal Regulations and reproduced in a note to Title 5, United States Code, Section 7301.

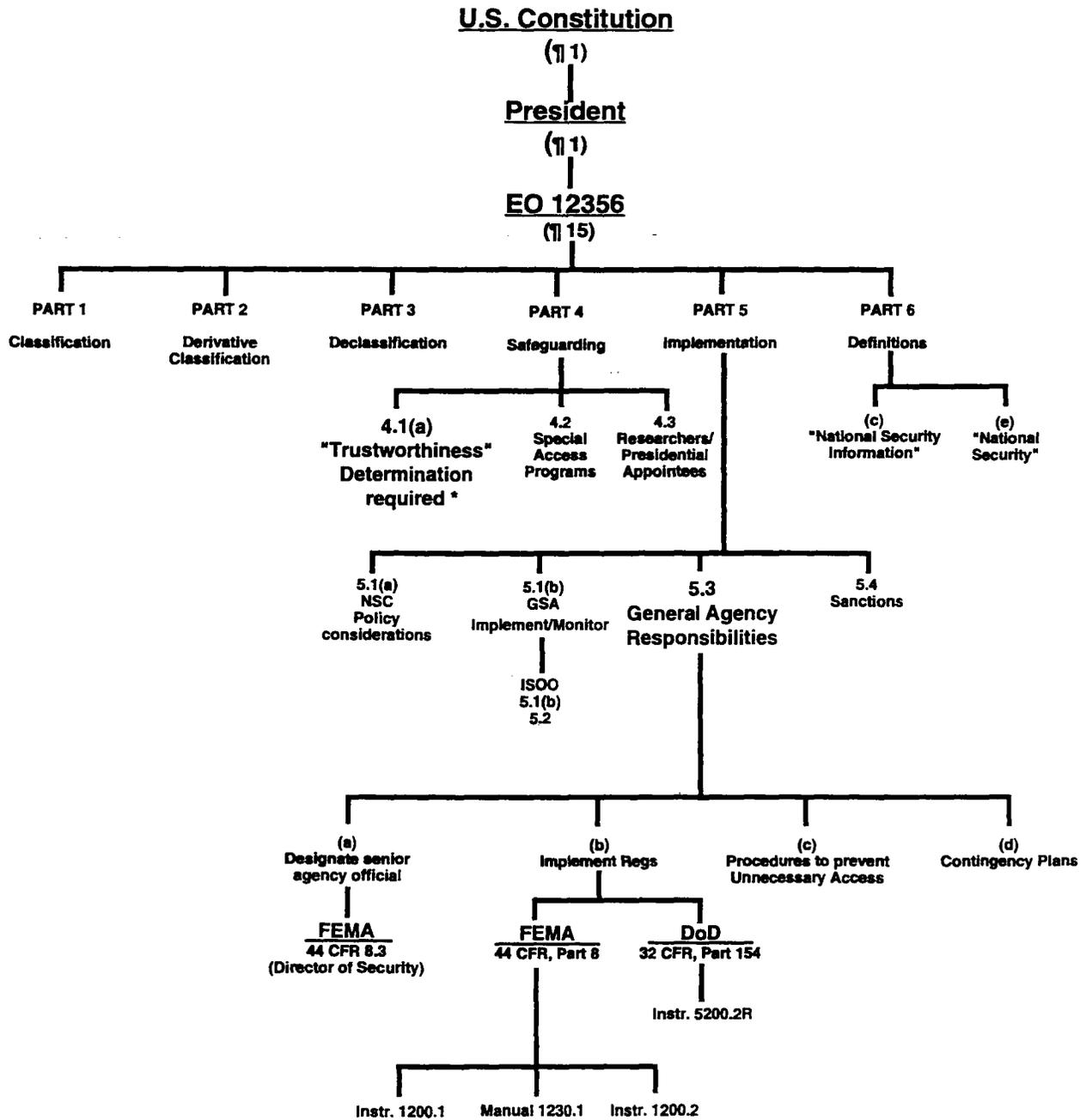
The synopsis also omits any reference to National Security Directive 63, "Single Scope Background Investigations," that was signed by President Bush on October 21, 1991, and directed that a "single scope background investigation" be used as the minimum investigative standard by all Executive branch departments and agencies for granting individuals access to Top Secret national security information and Sensitive Compartmented Information (SCI).

SCHEMATIC FOR EO 10450 / 5 CFR Part 732 AUTHORITIES



* NOTE: No authority given in EO 10450 to OPM to define "sensitive positions" or "national security positions" (5 CFR 732.101, .102).

SCHEMATIC FOR EXECUTIVE ORDER 12356



* NOTE: OPM has no special rule making or oversight responsibility, but see 5 CFR 732.102(a)(2) (definition of a "National Security Position").

RULE MAKING AUTHORITIES RELIED UPON BY
THE OFFICE OF PERSONNEL MANAGEMENT TO
PROMULGATE 5 CFR, PARTS 731, 732, & 736

TYPE OF AUTHORITY \ PART	731		732		736	
	Old	New	Old	New	Old	New
<u>STATUTORY</u>						
5 U.S.C. § 3301 ¹	X	X	X	X		
5 U.S.C. § 3302 ²	X	X	X	X		
5 U.S.C. § 7301 ³	X	X				
5 U.S.C. § 7312 ⁴			X	X		
5 U.S.C. § 7701 ⁵		X				
50 U.S.C. § 403 ⁶			X	X		
5 U.S.C. § 552a ⁷					X	X
5 U.S.C. § 1302 ⁸		X				
<u>EXECUTIVE ORDERS</u>						
E.O. 10577 ⁹ (5 C.F.R., Parts 1-8)	X	X	X			
E.O. 11222 ¹⁰	X	X				
E.O. 10450 ¹¹			X	X		
E.O. 11491 ¹²		X				
E.O. 12356 ¹³						
E.O. 10865 ¹⁴						
E.O. 12333 ¹⁵						

Note: On April 23, 1991, The Office of Personnel Management (OPM) announced in the Federal Register (56 FR 18650) the revision of its "Suitability" regulation (5 CFR Part 731), its "Personnel Security" regulation (5 CFR Part 732), and its "Investigations" regulation (5 CFR Part 736), in the form of "interim final regulations." These "new" regulations or rules have been codified in the January 1, 1992 edition of the Code of Federal Regulations (CFR). Copies of these "new" regulations are provided in Enc 8. A brief summary of these regulations is included in Enc 5, subparagraphs 20.c, d, and e.

These changes were made in response to various concerns expressed by members of Congress and various organizations over the

administration of the personnel security program. The "new" rules, in contrast to the "old" rules, are designed to make clearer distinctions between "suitability" requirements, which involve issues of government "efficiency", and "personnel security" requirements which involve certain additional issues relating to "national security" that are governed by Executive Order 10450 (Enc 6).

Footnotes to Enclosures 1, 2, and 3 to Tab E

1. 5 USC 3301.
(Enc 5, ¶3.a.)

Authorizes the President to prescribe regulations for the admission of individuals into the civil service as will best promote efficiency of civil service; to ascertain fitness of applicants as to age, health, character, knowledge, and ability for employment; and to appoint and prescribe duties of individuals to make inquiries for purposes of section.

Cited as authority in Executive Orders 10577⁹, 10450¹¹, and 11491¹².

Cited as authority in 5 CFR Parts 731, 732.

2. 5 USC 3302.
(Enc 5, ¶3.b.)

Authorizes the President to prescribe rules governing the competitive service to include necessary exceptions of positions from the competitive service.

Cited as authority in Executive Order 10577⁹, 10450¹¹.

Cited as authority in Parts 731 and 732.

3. 5 USC 7301.
(Enc 5, ¶3.a.)

Authorizes the President to prescribe regulations for the conduct of employees in the executive branch.

The President's authority to establish regulations was delegated to OPM and Office of Government Ethics, ^{10note} as appropriate by section 403 of EO 12674 of April 12, 1989.

Cited as authority in EO's 10577⁹, 10450¹¹, 11491¹².

Cited as authority in 5 CFR Part 731.

4. 5 USC 7312.
(Enc 5, ¶4)

Allows employees removed under 5 USC 7532 to be employed in another Federal agency.

Cited as authority in EO 10450¹¹.

Cited as authority in 5 CFR Part 732.

5. 5 USC 7701.

Establishes procedures for appeals to the Merit Systems Protection Board.

Cited as authority in 5 CFR Part 731.

6. 50 USC 403.
(Enc 5, ¶2)

Establishes the CIA under the NSC. Authorizes termination of employment "in the interest of the United States."

Cited as authority in 5 CFR Part 732.

7. 5 USC 5552a.

Privacy Act authority. Duties on agencies.

Cited as only authority in 5 CFR Part 736.

8. 5 USC 1302.
(Enc 5, ¶3.b.)

Authorizes OPM, subject to rules prescribed by the President for administration of the competitive service, to prescribe regulations for examinations for the competitive service.

Cited as authority in 5 CFR Part 731.

9. EO 10577, as amended
(Enc 5, ¶11)

"Amending the Civil Service Rules. . . ." 3 CFR, 1954-1958 Comp., p. 218; 5 USC 3301 note; 5 CFR Parts 1-8 (Civil Service Rules).

Authority for EO: 5 USC 3301¹, 7301³, 3302²; 3 USC 301.

10. EO 11222, as amended
(Enc 5, ¶13)

"Prescribing Standards of Ethical Conduct for Government

Officers and Employees," 3 CFR, 1964-1965 Comp., p. 306; 18 USC 201 note.

Authority for EO: President; 3 USC 301; [5 USC 7301³].

Note: EO 11222 was superseded by EO 12674 of April 12, 1989, "Principles of Ethical Conduct for government officer's and employees" 3 CFR , 1989 Comp., p. 215; 5 USC 7301 note. Authority for new EO: President and unspecified law of U.S.

11. EO 10450, as amended,
(Enc 5, ¶10; N)

"Security Requirements for Government Employment,"
3 CFR, 1949-1953 Comp., p. 936; 5 USC 7311 note.

Authority for EO: 5 USC 3301¹, 7301³; 5 USC 1101 et seq (Enc 5, ¶3.b.); 5 USC 3333, 7311 (Enc 5, ¶7); 5 USC 7531-7533, 3571, 5596, 7312⁴ (Enc 5, ¶4).

12. EO 11491, as amended

"Labor-Management Relations in the Federal Service,"
3 CFR 1966-1970 Comp., p. 861; 5 USC 7101 note.

Authority for EO: 5 USC 3301¹, 7301³.

SYNOPSIS OF PERSONNEL SECURITY AUTHORITIES

1. U.S. Constitution, as amended, Article II Section 1, Clause 1, vests "the executive power" in the President. Section 2, Clause 1, makes the President "Commander in Chief" of the Army and Navy of the United States [Armed Forces].

According to the U.S. Supreme Court, Article II of the Constitution gives the President authority "to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive branch that will give that person access to such information...." See Department of the Navy v. Egan, 108 S. Ct. 818, 824 (1988), and cases cited therein. (Note: this case upheld a "for cause" removal of a civilian laborer at a Trident facility after the denial of his security clearance in accordance with the adverse action provisions of the Civil Service Reform Act of 1978 (5 U.S.C. 7513), which did not allow the Merit Systems Protection Board to review the merits of a decision denying a security clearance.)

2. National Security Act of 1947, as amended, 50 U.S.C. 401 et seq. Section 2 of this Act (50 U.S.C. 401) establishes a statutory policy or framework for a comprehensive program to protect the national security. Thus, it may provide indirect authorization for various personnel security programs, including the security classification system under Executive Order 12356, which does not, however, specifically cite any statutory authority for its issuance. See 15, infra.

3. Civil Service Acts (5 U.S.C. 1101 et seq.).

a. Act of March 3, 1871, as amended, 5 U.S.C. 3301, 7301. Section 9 of this Act (16 Stat. 514) authorizes the President to prescribe regulations for the admission of individuals into the civil service; to ascertain the fitness of applications for the civil service; and to appoint and prescribe the duties of individuals to make inquiries for the above purposes (5 U.S.C. 3301). It also authorizes the President to prescribe regulations for the conduct of employees in the Executive branch (5 U.S.C. 7301).

b. Civil Service Act of 1883 (Pendleton Act), as amended, 5 U.S.C. 1101 et seq. Section 2 of this Act (22 Stat. 403), among other things, authorizes the President to prescribe rules governing the competitive service (5 U.S.C. 3302) and authorizes OPM to prescribe regulations regarding the competitive service (5 U.S.C. 1302).

c. The Civil Service Reform Act of 1978, as amended, 5 U.S.C. 1101 et seq.. This Act (92 Stat. 1111) contains the most recent substantive and procedural changes to the Civil Service Acts. See also Reorganization Plan No. 2 of 1978, 92 Stat. 3783 (establishing the Office of Personnel Management (OPM) and reforming the Personnel Management System).

4. Act of August 26, 1950, as amended, 5 U.S.C. 7531-7533, 3571, 5596, 7312. Section 1 of this Act (64 Stat. 476) gives the heads of certain agencies engaged in sensitive activities certain summary suspension and unreviewable dismissal powers over their civilian employees when deemed necessary "in the interest of the national security of the United States" (50 U.S.C. 7532), subject to certain reinstatement and reemployment provisions (5 U.S.C. 3571, 5596, 7312). The designated statutory agencies are the Departments of State, Commerce, Justice, and Defense. Other designated agencies are the military departments, the Coast Guard, the Atomic Energy Commission (Department of Energy/Nuclear Regulatory Commission), and NASA (5 U.S.C. 7531(1)-(8)). Section 3 of the Act (5 U.S.C. 7531(9)) also authorizes the President to apply its provisions to "such other agency of the government of the United States as the President designates in the best interest of national security." Three additional designations were made in 1988 by Presidential Memoranda (53 FR 26023) so that the National Security Agency, the Defense Intelligence Agency, and the Defense Mapping Agency are also covered by the summary suspension and dismissal provisions of the Act. While section 1 of Executive Order 10450 applies the Act to all other departments and agencies of the Government, the Supreme Court held in 1956 that the Act can only apply to "sensitive" or "national security" positions. Cole v. Young, 351 U.S. 536, 76 S. Ct. 861 (food and drug inspector's dismissal not authorized by Act). It did not expressly decide, however, that section 1 of Executive Order 10450 was an invalid extension of the Act to agencies not specified in the Act. *Ibid.* But see Editorial note 1, at p. 47 of the Office of Federal Register's 1989 Codification of Presidential Proclamations and Executive Orders (section 1 of Executive order held invalid by Supreme Court if applied to every department and agency).

The Act is intended to address the problem of "loyal" employees who are "so careless as to jeopardize the national security" and is not supposed to deal with disloyal employees who are already subject to a loyalty or personnel security program (Executive Order 9835 (1947) and its successor, Executive Order 10450 (1953)). See Senate Rept. No. 2158, July 25, 1950, accompanying H.R. 7439, 1950 U.S. Code Cong. Serv. 3278.

Summary removal procedures have also been given to the Director of the Central Intelligence Agency (50 U.S.C. 403(c)) and to the Secretary of Defense with respect to National Security Agency (NSA) employees (50 U.S.C. 833). However, the provisions of 5 U.S.C. 833 and 5 U.S.C. 7532 are not the exclusive means for

removing NSA employees. See Carlucci v. Doe, 109 S. Ct. 407, 411 (1988) (allowing "for cause" discharge of excepted service, nonveteran NSA technician pursuant to NSA personnel regulations promulgated under provisions of the National Security Agency Act of 1959, as amended, 50 U.S.C. 402 note).

5. Federal Civil Defense Act of 1950, as amended, 50 U.S.C. App. 2251 et seq. Section 403(a) of this Act (50 U.S.C. App. 2255(a)) establishes full field investigation requirements for those employees of the Federal Emergency Management Agency (FEMA), as a successor to the Federal Civil Defense Administration, who occupy positions "of critical importance from the standpoint of national security." It contains no waiver provision in the event of war, enemy attack, or any other emergency. In an undated memorandum [circa 1976] the Office of Legislative Affairs, Dept. of Justice, recommended repeal of the Loyalty Oath provision in section 403(b) of the Act (50 U.S.C. App. 2255(b)).

6. Act of April 5, 1952, as amended, 5 U.S.C. 1304. This Act (66 Stat. 43) assigns certain loyalty and security investigations to OPM with respect to employees identified in 22 U.S.C. 272b, 282b(e) and 290a who are assigned to certain international organizations. It contains no emergency waiver provisions.

7. Act of August 9, 1955, as amended, 5 U.S.C. 3333, 7311. This Act (69 Stat. 624) replaced Section 9A of the Hatch Act of 1939 (53 Stat. 1148) and requires a loyalty affidavit from a Government employee with an exception for certain "emergency" workers.

8. Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011 et seq. Sections 145 and 161 of this Act (42 U.S.C. 2165, 2201) establish specific personnel security investigation requirements for the Department of Energy, as a successor to the Atomic Energy Commission, before certain employees can have access to "restricted data" and "special nuclear materials." Section 145(h) allows access to restricted data pending an investigation report whenever war has been declared or "in the event of a national disaster due to enemy attack," as long as certain findings are made. Other sensitive agencies are also governed by special personnel security investigation requirements. The National Security Agency (NSA), for example, is allowed to temporarily employ persons and give them temporary access to classified information during a declared war or whenever the Secretary of Defense "determines that a national disaster exists," or in certain other "exceptional cases" upon the making of certain determinations (5 U.S.C. 832(a)). See also FPM chapter 732, Subchapter 1-2.c(special authorities).

9. Arms Control and Disarmament Act of 1961, as amended, 22 U.S.C. 2251 et seq. Section 45 of this Act (22 U.S.C. 2585) establishes certain personnel security and investigation requirements for persons working for the United States Arms Control and Disarmament Agency.

10. Executive Order 10450, April 27, 1953, as amended, "Security Requirements for Government Employment." This Order establishes the personnel security program for the Federal Government. It directs all Department and agency heads to establish and maintain an employee security program (section 2); requires all civilian appointments to be made subject to investigation whose scope depends on the sensitivity of the position, but allows certain exceptions to be made for certain types of employees (section 3(a)) or for sensitive positions during an emergency (section 3(b)); identifies certain categories of information to be developed during an investigation (section 8(a)); establishes a "security-investigations index" in OPM (section 9(a)); and revokes Executive Order 9835, March 21, 1947, "Prescribing Procedures for the Administration of an Employees Loyalty Program in the Executive Branch of the Government" (section 12). Some sections of this Order were expressly intended to implement the Act of August 26, 1950 (sections 1, 4, 5, 6, 7), supra. But the U.S. Supreme Court limited the scope of these provisions to "sensitive" or "national security" positions in Cole v. Young, supra. Other sections of the Order (sections 2, 3, 8, 9, 11, 14), which may also implement the President's "fitness" authority under the civil service laws (5 U.S.C. 3301, 3302), were not at issue in Cole v. Young, supra, and have not been limited to "sensitive" positions. OPM's new "interim final regulations," which implement the investigative authorities in Executive Order 10450, are at 5 CFR Part 732 (56 F.R. 18654 (April 23, 1991) and Federal Personnel Manual (FPM) Chapter 732 (under revision). Furthermore, as indicated in OPM's announcement of these regulations, the national security criteria established in Executive Order 10450 should no longer be used to determine "suitability" under 5 CFR Part 731 and FPM Chapter 731. See FPM Bulletins 736-21 (February 22, 1991) and 736-22 (May 9, 1991).

11. Executive Order 10577, November 23, 1954, as amended, "Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service." This Order (Part I) continues the delegation of the President's "fitness" authority (5 U.S.C. 3301) to the Director of OPM by means of the "Civil Service Rules," which are also codified in Title 5 of the CFR, Parts 1-8, and assign specific authorities, such as the authority to promulgate and enforce regulations (section 5.1(a)); to grant variations from the strict letter of the regulations under certain circumstances (section 5.1(b)); and to conduct investigations, including those that involve the qualifications and suitability of applicants for positions in the competitive service (section 5.2). The Order (Part III) also revokes Part II of Executive Order 9830, February 24, 1947, which was a prior amendment to the Civil Services Rules. OPM has further implemented Executive Order 10577 by promulgating certain regulations involving "suitability," which are at 5 CFR Part 731 and FPM Chapter 731, both of which are being revised to eliminate the "loyalty" criteria from 5 CFR §731.202(b) and FPM Chapter 731. See FPM Bulletins 736-21 and 736-22, supra.

12. Executive Order 10865, February 20, 1960, as amended, "Safeguarding Classified Information in Industry." This Order establishes policy and procedures concerning access to classified information by industrial representatives or contractors working for the Government. It contains no emergency waiver provisions. A proposed January 1989 Executive order on personnel security, entitled "Governing Access to Classified Information," which was prepared by an interagency committee pursuant to National Security Decision Directive (NSDD) 84 (1983), would have revoked sections 2 through 9 of Executive Order 10865. This draft order was soon withdrawn, however, in the face of severe criticisms from certain members of Congress and certain Federal employee and civil rights organizations. Section 3.2 of the draft order ("special circumstances") would have allowed for temporary access (up to 120 days) to classified national security information pending completion of the investigative and adjudicative process as long as the concerned agency head made certain findings and complied with certain procedures. Provision would also have been made for waiving a particular investigative procedure. No similar authority is contained in Executive Order 12356. See 15, *infra*.

13. Executive Order 11222, May 8, 1965, as amended, "Prescribing Standards of Ethical Conduct for Government Officers and Employees". This Order is an authority for suitability determinations pursuant to 5 CFR Part 731. Section 601 delegates regulation authority to OPM.

14. Executive Order 12333, December 4, 1981, "United States Intelligence Activities." This Order, among other things, requires certain agencies to establish "common security and access standards" for managing and handling foreign intelligence systems, information, and products (section 1.5(g)); and directs the CIA, DOD, and NSA to implement necessary investigations of certain persons and other security measures (sec. 1.8(h), 1.11(h), 1.12(b)(10)). FEMA is not a listed agency. See, however, FEMA, OGC July 1990 opinion.

15. Executive Order 12356, April 2, 1982, "National Security Information." This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. Section 6.1(e) defines "national security" as "the national defense or foreign relations of the United States." Section 4.1(a) requires all agency heads to "make a determination of trustworthiness" before a person is eligible for access to classified information. This Order does not include, however, any emergency waiver or access provisions. A proposed 1989 Executive order, "Governing Access to Classified Information", would have provided for temporary access. This draft order, for reasons indicated above, was withdrawn by April 1989. See 12, *supra*.

16. Executive Order 12564, September 15, 1986, "Drug Free Federal Workplace." This Order establishes certain policies and procedures for a drug testing program for any Government employee in a "sensitive position," which is defined to include persons that are in a position designated as Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive pursuant to Chapter 731 [sic] of the FPM or "sensitive" in accordance with Executive Order 10450 (section 7(d)(1)). Such position also includes an employee granted access to classified information pursuant to "a determination of trustworthiness" by an agency head in accordance with section 4 of Executive Order 12356 (section 7(d)(2)). Any other positions involving "national security" or other functions "requiring a high degree of trust and confidence" are also subject to the testing program (section 7(d)(5)). The Order contains no emergency waiver provision. OPM is directed to issue "government-wide guidance" to agencies on the implementation of the Order (section 6(a)(1)). Specific guidance on the drug testing program is contained in FPM Letter 792-19 (December 27, 1989); see also DoD Directive No. 1010.9 (August 23, 1988); 29 Government Employees Relations Report (GERR), "Special Report: Drug Testing" 416 (January 29, 1991); and NTEU v. Hallett, 756 F. Supp. 947 (E. D. La. 1991) (after remand from U.S. Supreme Court, authorizing use of drug tests for applicants to certain U.S. Customs Service positions requiring continued access to classified material.)

17. Executive Order 12656, November 18, 1988, "Assignment of Emergency Preparedness Responsibilities". This Order assigns specific "national security emergency" preparedness responsibilities to several Departments and agencies and replaces Executive Orders 10421 and 11490, as amended. It does not apply to certain telecommunications functions that are otherwise assigned by Executive Order 12472 (section 103(d)). It also does not constitute authority to implement any plans prepared pursuant to the Order (section 102(b)). With respect to personnel security matters, section 2201(3) directs the Office of Personnel Management to "[d]evelop plans to accommodate the surge of Federal personnel security background and pre-employment investigations during national security emergencies." A "national security emergency" is defined in section 101(a) as "any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States."

18. National Security Decision Directive 84, March 11, 1983, "Safeguarding National Security Information". This NSDD (paragraph 5) authorized the use of polygraph (lie detector) tests by the heads of all Federal agencies in Federal personnel security. The Government-wide polygraph test provision was never put into effect due to objections from Congress. See, e.g., 23 GERR 1162 (August 12, 1985). The Defense Department (DoD), however, has been allowed by Congress (since 1985) to conduct a pilot polygraph program for a specific number of persons. See, e.g., 24 Id. 99 (January 27,

1986); P.L. 100-180 (section 1121) and DoD Directive 5210.48 (1984) (includes a provision (par.12.e) allowing use of polygraph in determining "initial eligibility of foreign nationals for access to classified information"). DoD has also been given authority under section 7(b) of the Employee Polygraph Protection Act of 1988 (29 U.S.C. 2006 (b)) to give a lie detector test to any expert or consultant under DoD contract or any employee of a DoD contractor in the performance of any counterintelligence function. The Department of Energy has similar authority in connection with "atomic energy defense activities." Ibid. The Act also allows the use of a lie detector on any person applying for a position in the National Security Agency, the Defense Intelligence Agency, or the Central Intelligence Agency (29 U.S.C. 2006 (b)(2)(A)(iv)). This Act also exempts all Governments (U.S., State, and local) from the prohibitions of the Act (29 U.S.C. 2006(a)). This NSDD 84 also directed (paragraph 6) the establishment of an interdepartmental group to study the Federal personnel security program and to recommend appropriate revisions. In January 1989, the National Security Council circulated a draft Executive order on "Personnel Security" for final agency comments. It was withdrawn, however, a few months later after it was criticized and attacked by certain members of Congress and various Government employee and civil rights groups. See 12, supra. This critical response to the draft order has also resulted in certain changes to OPM's personnel security regulations. See 10, 11, supra.

19. OMB Circular A-130, December 12, 1985, "Management of Federal Information Resources." Appendix III of this Circular establishes certain minimum controls for the security of Federal Automated Information Systems and assigns certain security responsibilities, including personnel security procedures consistent with OPM policies (3.b., 4.d.). OMB published a proposed revision to the Circular on April 29, 1992 (57 FR 18296), but did not propose any immediate changes to Appendix III. It has plans, however, to publish revisions to Appendix III in the fall of 1992 that will incorporate requirements of the Computer Security Act of 1987 (Pub. L. 100-235, 101 Stat. 1724) and OMB Bulletin 90-08 and insure better coordination with OMB Circular A-123, "Internal Control Systems" (57 FR 18298).

20. Code of Federal Regulations (CFR). The only CFR references cited and described here are those of OPM (5 CFR Parts 5, 230, 731, 732, and 736) and DoD (32 CFR Part 154). The personnel security regulations of other agencies could also be examined for other restrictions and waiver authorities.

a. 5 CFR Part 5

(1) Section 5.1, which is a Presidential regulation (Executive Order 10577, as amended), authorizes the Director of OPM to promulgate and enforce regulations necessary to carry out the provisions of the Civil Service Act the Civil Service

Rules and to grant a variation from the strict letter of a regulation "whenever there are practical difficulties and unnecessary hardships in complying with the strict letter of the regulation" and certain other conditions apply. This authority, however, is probably intended only for the benefit of civil service employees who may, for example, be deprived of a job due to no fault on their part if OPM regulations would otherwise require dismissal or loss of status. Thus, it may not be available to relieve agencies from any personnel security investigative requirements of Executive Order 10450 and/or 5 CFR Part 732, especially when section 5.1 of the Civil Service Rules has no variance standard based on any "national security" interests.

(2) Section 5.2 authorizes the OPM Director to investigate the qualifications and suitability of applicants for positions in the competitive service. The first explicit authority for the conduct of suitability investigations was contained in the 1938 revisions to Rule III, section 3 of the Civil Service Rules. See Executive Order 7915, June 24, 1938.

b. 5 CFR Part 230. Subpart D (5 CFR §230.401) authorizes agencies, upon an attack on the United States, "to carry out whatever personnel activities may be necessary to the effective functioning of their organizations during a period of disaster without regard to any regulation or instruction of OPM, except those which become effective upon or following an attack on the United States." Subpart D (5 CFR §230.402) also authorizes the use of an "emergency indefinite" appointment authority in the event of a "national emergency," as defined by OPM.

c. 5 CFR Part 731 (Suitability). This Part, as amended (56 FR 18650-4 (interim final regulations)), establishes criteria and procedures for making determinations of suitability for employment in positions in the competitive service and for career appointments in the Senior Executive Service (SES) on the basis of the person's character or certain types of conduct. These determinations are distinct from those of eligibility for assignment to or retention in sensitive national security positions (5 CFR §731.101). Part 731 also refers to issuances of the Federal Personnel Manual System for specific policies, procedures, criteria and guidance on its implementation (5 CFR §731.102(b)). The new procedures include a revised, shorter "Questionnaire for Non-Sensitive Positions" (SF 85) and a new "Questionnaire for Public Trust Positions" (SF 85P). The former, disqualifying "suitability" factor ("reasonable doubt as to the loyalty of the person involved to the Government of the United States") in 5 CFR §731.202(b)(7) will be changed to "knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force."

d. 5 CFR Part 732 (National Security Positions). This Part, as amended (56 F.R. 18654-5 (interim final regulations)), establishes certain requirements and procedures which each agency shall observe for determining "national security positions" pursuant to Executive Order 10450 (5 CFR §732.101); sensitivity level designations and investigative requirements for sensitive positions, including referral to FPM Chapter 732 for investigative requirements (5 CFR §732.201); and waivers and exceptions to investigative requirements for such positions that are contained in sections 3(a) and 3(b) of Executive Order 10450 (5 CFR §732.202). The new OPM procedures include a revised "Questionnaire for Sensitive Positions" (SF 86), which covers a wider range of activities and associations and for longer time periods (up to 15 years) than either the revised SF 85 and the new SF 85P, mentioned above.

e. 5 CFR Part 736 (Personnel Investigations). This Part, as amended (56 F.R. 18655 (interim final regulations)), specifies certain requirements for personnel investigations which apply to both suitability and national security investigations under Parts 731 and 732 and other investigations to determine eligibility or qualifications not covered by Parts 731 and 732 of title 5 (5 CFR §736.101(a)). Subpart B contains a specific provision governing the "timing of investigations" (5 CFR §736.201(c)) that requires any required investigations to be initiated within 14 days of placement except for "Critical-Sensitive" positions (must complete replacement unless there is "waiver" compliance (5 CFR §732.202(a))); and "Special-Sensitive" positions (must complete replacement; no waiver allowed). The new regulations also include a provision for the delegation by OPM of investigative authority upon request of an agency head (5 CFR §736.201(b)).

f. 32 CFR Part 154 (32 CFR §154.1 et seq.) This Part establishes security regulations for the Department of Defense (DoD). It is based on Executive Orders 10450, 12356, and 12333 and includes general waiver provisions "under combat conditions or other military exigencies" (32 CFR §154.2(d)). Certain persons are also authorized to waive investigative requirements concerning appointments to sensitive positions, assignments to sensitive duties, or access to classified information (32 CFR §154.20).

21. Federal Personnel Manual System

Chapter 171 (Subchapter 2) of the Federal Personnel Manual (FPM) states that the OPM System is "the official medium of the Office of Personnel Management (OPM) for issuing personnel instructions, operational guidance, policy statements, related material on government wide personnel programs, and advice on good practice in personnel management to other agencies." The "basic" FPM is a "component" of the FPM System and is written for personnel officials as a group. The FPM Supplements are another component of the FPM System and are written for "specialized audiences."

Thus, the distribution of the FPM and the Supplements will vary. The first FPM was issued in 1945; the latest version is based on a complete 1963 revision. (Note: the FPM System is not considered a means of promulgating official rules or regulations, which are published for comment in the Federal Register, included in the Code of Federal Regulations, and given greater deference or enforceability by the courts.)

a. Federal Personnel Manual (FPM).

(1) Chapter 230 (Organization of the Government for Personnel Management). Subchapter 4-3 establishes certain criteria for the use of the "emergency indefinite" appointment authority (5 CFR §230.402).

(2) Chapter 731 (Suitability). This Chapter provides guidance and establishes basic OPM requirements for investigating and adjudicating suitability for employment or continued employment in the competitive civil service. (Note: Further specifics TBD per draft of revised Chapter 731. See FPM Bulletin No. 736-21, par. 2 (February 22, 1991).)

(3) Chapter 732 (National Security Positions). This Chapter provides guidance on determining "national security positions" pursuant to Executive Order 10450 and establishes investigative requirements for each of three sensitivity levels identified in 5 CFR §732.201(a). (Note: Further specifics TBD per draft of revised Chapter 732. See FPM Bulletin No. 736-21, par. 3 (February 22, 1991).)

(4) Chapter 736 (Personnel Investigations). This Chapter provides guidance on general investigations processing and procedures. (Note: Further specifics TBD per draft of revised Chapter 736. See FPM Bulletin No. 736-21, par 4. (February 22, 1991).)

(5) Chapter 910 (Mobilization Readiness).

(a) Subchapter 1 provides general guidance on emergency readiness planning and preemergency operating instructions in certain areas of personnel management. It includes references to more specific guidance and instructions in FPM Supplement 910-1 (National Emergency Readiness of Federal Personnel Management) and FPM Supp. 990-3 (National Emergency Standby Regulations).

(b) Subchapter 2 provides guidance on and permits preappointment investigations of national emergency "standby" recruits, to include modified preliminary screening for those selected for Non-Sensitive positions. Agencies requesting such investigations are referred to FPM Supp. 296-33 (The Guide to Processing Personnel Actions).

b. FPM Supplement 910-1
(National Emergency Readiness of Federal Personnel Management).

(1) Book I, Chapter 2 (OPM Plans for Federal Personnel Management in National Emergency).

Subchapter D (Plan for General War) of Chapter 2 provides that in the event of a general war, including an attack on the United States: (a) OPM "will have broad authority to suspend civilian personnel laws, orders, rules, and regulations" (D. 1); (b) OPM will curtail limited suitability investigations; suspend qualifications investigations; suspend temporarily the national agency checks and inquiry process (D. 29); (c) agencies will conduct qualifications and limited suitability investigations when necessary (D.30); (d) agencies will have authority to defer [sensitive or national security] investigations required under section 3 of Executive Order 10450 (D. 31); and (e) certain appeals requirements will be suspended (D. 32).

(2) Book I, Chapter 3 (Agency Planning for Emergency Personnel Management).

This Chapter establishes certain general criteria for an agency's personnel management plan for use in an emergency; but it contains no specific criteria concerning security investigations by agencies.

(3) Book II, Subchapter S731 (Suitability).

This Subchapter would only suspend the suitability appeal requirements (Subpart D [E]) of 5 CFR Part 731 by means of Part M-731 of FPM Supp. 990-3. (Note: this Part will need revision based on new regulations.)

(4) Book II, Subchapter S732 (Personnel Security and Related Programs).

This Subchapter would only suspend appeal authorizations for certain formerly separated employees (subpart D) of 5 CFR Part 732 (5 CFR §732.401) by means of Part M-732 of FPM Supp. 990-3.

(5) Book II, Subchapter S736 (Investigations).

This Subchapter provides for the modification of OPM's investigation program in the event of an attack by reassigning investigative personnel to the field so that each agency will have expanded authority to conduct their own investigations. Other OPM "adjustments" include the discontinuance of "qualifications investigations" for high level job applicants (S736-2); discontinuance of "limited suitability investigations" for non-sensitive position appointees, but continue to refer "loyalty" questions to the FBI (S736-4); deferral or temporary

discontinuance of the investigative requirements of subsection 3(a) of Executive Order 10450 "until conditions permit" continuance of the required investigations (S736-5); allowing agencies to make appointments to non-sensitive positions without regard to the requirements of section 3(a) of Executive Order 10450 under certain conditions by means of standby regulation M-736.101 in FPM Supp. 990-3 (S736-6); and allowing an agency head to fill a sensitive position for a limited period in an emergency, as allowed by section 3(b) of Executive Order 10450; and to delegate this authority by means of standby regulation M-736.102 in FPM Supp. 990-3 (S736-7). (Note: these standby regulations will need revision in view of new regulations and transfer of authorities to 5 CFR Part 732.)

c. FPM Supplement 990-3 (National Emergency Standby Regulations-Personnel and Manpower).

In the event of an "attack," the following would apply:

(1) Part M-731 (Suitability) would only suspend Subpart D [E] of 5 CFR Part 731, which allows appeals to the Merit Systems Protection Board by any applicant or eligible who is disqualified from examination or appointment by OPM for any reason stated in 5 CFR §731.202.

(2) Part M-732 (Personnel Security and Related Programs) would only suspend Subpart D of 5 CFR Part 732, which concerns reemployment eligibility of certain former Federal employees (5 CFR §732.401).

(3) Part M-736 (Investigations) would add a new part M-736 to 5 CFR that would allow agencies to defer for limited periods the initiation of investigations required under subsection 3(a) of Executive Order 10450 (M-736.101) and allow an agency head to delegate his authority under subsection 3(b) of the same Order to fill "sensitive" positions without a completed preappointment investigation (M-736.102). (Note: this Part will need revision due to redeployment of regulatory provisions to Part 732.)

Executive Order 10450—Security requirements for Government employment

SOURCE: The provisions of Executive Order 10450 of Apr. 27, 1953, appear at 18 FR 2489, 3 CFR, 1949-1953 Comp., p. 936, unless otherwise noted.

WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632, *et seq.*); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64 Stat. 476 (5 U.S.C. 22-1, *et seq.*), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

SECTION 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government. ¹

SEC. 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

¹ EDITORIAL NOTE: In *Cole v. Young*, 76 S.Ct. 861 (1955), section 1 of EO 10450 was held to be invalid if applied to every department and agency.

Codification of Presidential Proclamations and Executive Orders

SEC. 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: *Provided*, that upon request of the head of the department or agency concerned, the Office of Personnel Management may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such person a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has been conducted: *Provided*, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: *And provided further*, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field pre-appointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

[Sec. 3 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 of March 21, 1947, and, after such further investigation as may be appropriate, shall re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

SEC. 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his

Chapter 5—Federal Civilian Personnel

representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

SEC. 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

SEC. 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be reinstated or restored to duty or reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: *Provided*, that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Office of Personnel Management that such person is eligible for such employment.

[Sec. 7 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, sexual perversion.

(iv) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.

Codification of Presidential Proclamations and Executive Orders

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates 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.

(4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices 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, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

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

(8) Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct.

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Office of Personnel Management, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Office. The Office shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Office of Personnel Management, and other departments and agencies may use such facilities under agreement with the Office.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests

Chapter 5—Federal Civilian Personnel

of the national security, or information relating to any of the matters described in subdivisions (2) through (8) of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

[Sec. 8 amended by EO 10491 of Oct. 13, 1953, 18 FR 6583, 3 CFR, 1949-1953 Comp., p. 973; EO 10531 of May 27, 1954, 19 FR 3069, 3 CFR, 1954-1958 Comp., p. 193; EO 10548 of Aug. 2, 1954, 19 FR 4871, 3 CFR, 1954-1958 Comp., p. 200; EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 9. (a) There shall be established and maintained in the Office of Personnel Management a security-investigations index covering all persons as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Office under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Office of Personnel Management information appropriate for the establishment and maintenance of the security-investigations index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

[Sec. 9 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

SEC. 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards

Codification of Presidential Proclamations and Executive Orders

and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Office of Personnel Management on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion and the determination of the board shall be forwarded to the head of the department or agency concerned: *Provided*, that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Office of Personnel Management on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

[Sec. 11 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 12. Executive Order No. 9835 of March 21, 1947, as amended, is hereby revoked.

[Sec. 12 amended by EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874]

SEC. 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an appropriate employee-security program.

SEC. 14. (a) The Office of Personnel Management, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which this order is being implemented by the departments and agencies of the Government for the purpose of determining:

(1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.

(2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Office of Personnel Management shall report to the National Security Council, at least semiannually, on the results of such study, shall recommend means to correct any such deficiencies or tendencies, and shall inform the National Security Council immediately of any deficiency which is deemed to be of major importance.

(b) All departments and agencies of the Government are directed to cooperate with the Office of Personnel Management to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

(c) To assist the Office of Personnel Management in discharging its responsibilities under this order, the head of each department and agency shall, as soon as possible and in no event later than ninety days after receipt of the final investigative report on a civilian officer or employee subject to a full field investigation under the provisions of this

Chapter 5—Federal Civilian Personnel

order, advise the Office as to the action taken with respect to such officer or employee. The information furnished by the heads of departments and agencies pursuant to this section shall be included in the reports which the Office of Personnel Management is required to submit to the National Security Council in accordance with subsection (a) of this section. Such reports shall set forth any deficiencies on the part of the heads of departments and agencies in taking timely action under this order, and shall mention specifically any instances of noncompliance with this subsection.

[Sec. 14 amended by EO 10550 of Aug. 5, 1954, 19 FR 4981, 3 CFR, 1954-1958 Comp., p. 200; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 15. This order shall become effective thirty days after the date hereof.

Executive Order 12356—National security information

SOURCE: The provisions of Executive Order 12356 of Apr. 2, 1982, appear at 47 FR 14874 and 15557, 3 CFR, 1982 Comp., p. 166, unless otherwise noted.

TABLE OF CONTENTS

	<i>Page</i>
PREAMBLE	[651]
PART 1. <i>Original Classification</i>	
1.1 Classification Levels.....	[651]
Chapter 32—National Defense	
1.2 Classification Authority.....	[652]
1.3 Classification Categories.....	[654]
1.4 Duration of Classification.....	[655]
1.5 Identification and Markings.....	[655]
1.6 Limitations on Classification.....	[655]
PART 2. <i>Derivative Classification</i>	
2.1 Use of Derivative Classification.....	[656]
2.2 Classification Guides.....	[656]
PART 3. <i>Declassification and Downgrading</i>	
3.1 Declassification Authority.....	[657]
3.2 Transferred Information.....	[657]
3.3 Systematic Review for Declassification.....	[657]
3.4 Mandatory Review for Declassification.....	[658]
PART 4. <i>Safeguarding</i>	
4.1 General Restrictions on Access.....	[659]
4.2 Special Access Programs.....	[659]
4.3 Access by Historical Researchers and Former Presidential Appointees.....	[660]
PART 5. <i>Implementation and Review</i>	
5.1 Policy Direction.....	[660]
5.2 Information Security Oversight Office.....	[660]
5.3 General Responsibilities.....	[661]
5.4 Sanctions.....	[662]
PART 6. <i>General Provisions</i>	
6.1 Definitions.....	[662]
6.2 General.....	[663]

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

PART 1

Original Classification

SECTION 1.1 *Classification Levels.*

(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Codification of Presidential Proclamations and Executive Orders

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

SEC. 1.2 Classification Authority. ¹

¹ EDITORIAL NOTE: On May 7, 1982, the President issued an order of designation (47 FR 20105, 3 CFR, 1982 Comp., p. 257) the text of which follows:

Pursuant to the provisions of Section 1.2 of Executive Order No. 12356 of April 2, 1982, entitled "National Security Information," I hereby designate the following officials to classify information originally as "Top Secret", "Secret", or "Confidential":

TOP SECRET

Executive Office of the President:

The Vice President
The Counsellor to the President
The Chief of Staff and Assistant to the President
The Deputy Chief of Staff and Assistant to the President
The Director, Office of Management and Budget
The United States Trade Representative
The Assistant to the President for National Security Affairs
The Director, Office of Science and Technology Policy
The Chairman, The President's Foreign Intelligence Advisory Board
The Chairman, The President's Intelligence Oversight Board

The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Secretary of the Army
The Secretary of the Navy
The Secretary of the Air Force
The Attorney General
The Secretary of Energy
The Chairman, Nuclear Regulatory Commission
The Director, United States Arms Control and Disarmament Agency
The Director of Central Intelligence
The Administrator, National Aeronautics and Space Administration
The Administrator of General Services
The Director, Federal Emergency Management Agency

SECRET

Executive Office of the President:

The Chairman, Council of Economic Advisers
The President's Personal Representative for Micronesian Status Negotiations
The Secretary of Commerce
The Secretary of Transportation
The Administrator, Agency for International Development
The Director, International Communication Agency

Chapter 32—National Defense

(a) *Top Secret*. The authority to classify information originally as Top Secret may be exercised only by:

- (1) the President;
- (2) agency heads and officials designated by the President in the FEDERAL REGISTER; and
- (3) officials delegated this authority pursuant to Section 1.2(d).

(b) *Secret*. The authority to classify information originally as Secret may be exercised only by:

- (1) agency heads and officials designated by the President in the FEDERAL REGISTER;
- (2) officials with original Top Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

(c) *Confidential*. The authority to classify information originally as Confidential may be exercised only by:

- (1) agency heads and officials designated by the President in the FEDERAL REGISTER;
- (2) officials with original Top Secret or Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

(d) *Delegation of Original Classification Authority*.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1),¹ provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1),¹ provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1),¹ provided that official has been delegated original classification authority by the agency head.

CONFIDENTIAL

The President, Export-Import Bank of the United States
The President, Overseas Private Investment Corporation
The Administrator, Environmental Protection Agency

Any delegation of this authority shall be in accordance with Section 1.2(d) of the Order.

This Order shall be published in the FEDERAL REGISTER.

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

Codification of Presidential Proclamations and Executive Orders

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

SEC. 1.3 Classification Categories.

(a) Information shall be considered for classification if it concerns:

- (1) military plans, weapons, or operations;
- (2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
- (3) foreign government information;
- (4) intelligence activities (including special activities), or intelligence sources or methods;
- (5) foreign relations or foreign activities of the United States;
- (6) scientific, technological, or economic matters relating to the national security;
- (7) United States Government programs for safeguarding nuclear materials or facilities;
- (8) cryptology;
- (9) a confidential source; or
- (10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or in-

Chapter 32—National Defense

advertent or unauthorized disclosure in the United States or abroad of identical or similar information.

SEC. 1.4 *Duration of Classification.*

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

SEC. 1.5 *Identification and Markings.*

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

- (1) one of the three classification levels defined in Section 1.1;
- (2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;
- (3) the agency and office of origin; and
- (4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

SEC. 1.6 *Limitations on Classification.*

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to

Codification of Presidential Proclamations and Executive Orders

prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1),¹ or an official with original Top Secret classification authority.

PART 2

Derivative Classification

SEC. 2.1 Use of Derivative Classification.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

SEC. 2.2 Classification Guides.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a)(1);¹ and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

Chapter 32—National Defense

(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

PART 3

Declassification and Downgrading

SEC. 3.1 Declassification Authority.

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).¹

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

SEC. 3.2 Transferred Information.

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

SEC. 3.3 Systematic Review for Declassification.

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

Codification of Presidential Proclamations and Executive Orders

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

SEC. 3.4 *Mandatory Review for Declassification.*

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

- (1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and
- (2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order.

Chapter 32—National Defense

They shall release this information unless withholding is otherwise authorized under applicable law.

(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

PART 4

Safeguarding

SEC. 4.1 General Restrictions on Access.

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

SEC. 4.2 Special Access Programs.

Codification of Presidential Proclamations and Executive Orders

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.

(b) Each ~~agency head shall~~ establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

SEC. 4.3 Access by Historical Researchers and Former Presidential Appointees.

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

(1) are engaged in historical research projects, or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

PART 5

Implementation and Review

SEC. 5.1 Policy Direction.

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

SEC. 5.2 Information Security Oversight Office.

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

(b) The Director shall:

Chapter 32—National Defense

(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

(2) oversee agency actions to ensure compliance with this Order and implementing directives;

(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) ¹ may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;

(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

SEC. 5.3 *General Responsibilities.*

Agencies that originate or handle classified information shall:

(a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the FEDERAL REGISTER to the extent that these regulations affect members of the public;

(c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the mini-

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

Codification of Presidential Proclamations and Executive Orders

mum consistent with operational and security requirements and needs; and

(d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

SEC. 5.4 Sanctions.

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official designated under Section 5.3(a)(1)¹ so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) Each agency head or the senior official designated under Section 5.3(a)(1)¹ shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b) (1) or (2) occurs.

PART 6

General Provisions

SEC. 6.1 Definitions.

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or govern-

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

Chapter 32—National Defense

ments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(e) "National security" means the national defense or foreign relations of the United States.

(f) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

SEC. 6.2 *General.*

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order.

(e) This Order shall become effective on August 1, 1982.

code of federal regulations

Administrative Personnel

*See Parts
731, 732, 736*

5

PARTS 700 TO 1199

Revised as of January 1, 1992

CONTAINING
A CODIFICATION OF DOCUMENTS
OF GENERAL APPLICABILITY
AND FUTURE EFFECT

As of January 1, 1992

With Ancillaries

Published by
the Office of the Federal Register
National Archives and Records Administration

as a Special Edition of
the Federal Register



PART 731—SUITABILITY

Subpart A—Scope

- Sec.
 731.101 Purpose.
 731.102 Implementation.
 731.103 Delegation to agencies.

Subpart B—Suitability Determinations

- 731.201 Standard.
 731.202 Criteria.

Subpart C—Suitability Rating Actions

- 731.301 Jurisdiction.
 731.302 Risk designation and investigative requirements.
 731.303 Actions by OPM and other agencies.
 731.304 Debarment.

Subpart D—Suitability Actions

- 731.401 Scope.
 731.402 Notice of proposed action.
 731.403 Answer.
 731.404 Decision.

Subpart E—Administrative Review and Appeal

- 731.501 OPM Review Panel.
 731.502 Procedures.
 731.503 Content of appeal.
 731.504 Representation.
 731.505 Pay status.
 731.506 Decision.
 731.507 Scope of review.
 731.508 Appeal to the Merit Systems Protection Board.

Subpart F—Reemployment Eligibility

- 731.601 Reemployment eligibility of certain former Federal employees.

Subpart G—Savings Provision

- 731.701 Savings provision.

AUTHORITY: 5 U.S.C. 1302, 3301, 3302, 7301, 7701; E.O. 10577, 3 CFR, 1954-1958 Comp., p. 218; E.O. 11222, 3 CFR, 1964-1965 Comp., p. 306.; E.O. 11491, 3 CFR, 1966-1970 Comp., p. 861.

SOURCE: 56 FR 18650, Apr. 23, 1991, unless otherwise noted.

Subpart A—Scope

- § 731.101 Purpose.

The purpose of this part is to establish criteria and procedures for making determinations of suitability for employment in positions in the competitive service and for career ap-

pointments in the Senior Executive Service (hereinafter in this part, "competitive service") pursuant to 5 U.S.C. 3301 and E.O. 10577. Section 3301 of title 5, United States Code, directs consideration of "age, health, character, knowledge, and ability for the employment sought." E.O. 10577 directs OPM to examine "suitability" for competitive Federal employment. This part concerns only determinations of "suitability" based on an individual's character or conduct that may impact the efficiency of the service by jeopardizing an agency's accomplishment of its duties or responsibilities, or by interfering with or preventing effective service in the position applied for or employed in, and determinations that there is a statutory or regulatory bar to employment. Determinations made under this part are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions made under E.O. 10450 or similar authorities.

§ 731.102 Implementation.

(a) An investigation conducted for the purpose of determining suitability under this part may not be used for any other purpose except as provided in a Privacy Act system of records notice published by the agency conducting the investigation.

(b) Policies, procedures, criteria, and guidance for the implementation of this part shall be set forth in issuances of the Federal Personnel Manual System or other appropriate instruments. Agencies exercising authority under this part by delegation from OPM shall conform to such policies, procedures, criteria, and guidance.

§ 731.103 Delegation to agencies.

(a) *Direct Hires.* The head of each agency is delegated authority for adjudicating suitability under this part for applicants filing directly with the agency outside a civil service register.

(b) OPM may in its discretion delegate to the heads of agencies authority for adjudicating suitability in other cases involving applicants and eligibles for, and appointees to, competitive service positions in the agency.

(c) Paragraphs (a) and (b) of this section notwithstanding, OPM may exercise its jurisdiction under this part in any case when deemed necessary.

(d) Any applicant, eligible, or appointee who is found unsuitable by any agency having delegated authority from OPM under this part for any reason named in § 731.202 may appeal to the Merit Systems Protection Board under the Board's regulations.

Subpart B—Suitability Determinations

§ 731.201 Standard.

Subject to subpart C of this part, OPM may deny an applicant examination, deny an eligible appointment, and direct an agency to remove an appointee or employee when OPM determines the action will promote the efficiency of the service.

§ 731.202 Criteria.

(a) *General.* In determining whether its action will promote the efficiency of the service, OPM or an agency to which OPM has delegated authority under § 731.103 of this chapter, shall make its determination on the basis of:

(1) Whether the conduct of the individual may reasonably be expected to interfere with, or prevent, efficient service in the position applied for or employed in; or

(2) Whether the conduct of the individual may reasonably be expected to interfere with, or prevent, effective accomplishment by the employing agency of its duties or responsibilities; or

(3) Whether a statutory or regulatory bar prevents the lawful employment of the individual in the position in question.

(b) *Specific factors.* When making a determination under paragraph (a) of this section, any of the following reasons may be considered a basis for finding an individual unsuitable:

(1) Misconduct or negligence in prior employment which would have a bearing on efficient service in the position in question, or would interfere with or prevent effective accomplishment by the employing agency of its duties and responsibilities;

(2) Criminal or dishonest conduct related to the duties to be assigned to the applicant or appointee, or to that person's service in the position or the service of other employees;

(3) Intentional false statement or deception or fraud in examination or appointment;

(4) Refusal to furnish testimony as required by § 5.4 of this chapter;

(5) Alcohol abuse of a nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others;

(6) Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;

(7) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force;

(8) Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

(c) *Additional considerations.* In making a determination under paragraphs (a) and (b) of this section, OPM and agencies shall consider the following additional factors to the extent that they deem these factors pertinent to the individual case:

(1) The kind of position for which the person is applying or in which the person is employed, including the degree of public trust or risk in the position;

(2) The nature and seriousness of the conduct;

(3) The circumstances surrounding the conduct;

(4) The recency of the conduct;

(5) The age of the person involved at the time of the conduct;

(6) Contributing societal conditions;

(7) The absence or presence of rehabilitation or efforts toward rehabilitation.

Subpart C—Suitability Rating Actions

§ 731.301 Jurisdiction.

(a) *Appointments subject to investigation.* (1) In order to establish an appointee's suitability for employment in the competitive service, every appoint-

ment to a position in the competitive service is subject to investigation by OPM, except:

- (i) Promotion;
- (ii) Demotion;
- (iii) Reassignment;
- (iv) Conversion from career-conditional to career tenure;

(v) Appointment, or conversion to an appointment, made by an agency of an employee of that agency who has been serving continuously with that agency for at least one year in one or more positions under an appointment subject to investigation; and

(vi) Transfer, provided the one-year, subject-to-investigation period applied to the previous appointment has expired.

(2) Appointments are subject to investigation to continue OPM's jurisdiction to investigate the suitability of an applicant after appointment and to authorize OPM to require removal when it finds the appointee is unsuitable for Federal employment. The subject-to-investigation condition may not be construed as requiring an employee to serve a new probationary or trial period or as extending the probationary or trial period of an employee.

(b) *Duration of condition.* The subject-to-investigation condition expires automatically at the end of one year after the effective date of appointment, except in a case involving intentional false statement or deception or fraud in examination or appointment, or refusal to furnish testimony.

§ 731.302 Risk designation and investigative requirements.

(a) *Risk designation.* Agency heads shall designate every competitive service position within the agency at either a High, Moderate, or Low risk level as determined by the position's potential for adverse impact to the efficiency of the service.

(b) *Investigative requirements.* Persons receiving an appointment made subject to investigation shall undergo a background investigation, the scope and coverage of which shall be determined by OPM in accordance with the level of risk determined by the agency.

(c) *Suitability reinvestigations.* (1) Every incumbent of a competitive service position:

(i) Designated High Risk under paragraph (a) of this section, or

(ii) That is a law enforcement or public safety position designated Moderate Risk under paragraph (a) of this section, shall be subject to a periodic reinvestigation of a scope established by OPM 5 years after placement, and at least once each succeeding 5 years.

(2) Periodic reinvestigations required by paragraph (c)(1) of this section may be adjudicated by the employing agency according to the procedures in this part, if applicable.

§ 731.303 Actions by OPM and other agencies.

(a) For a period of one year after the effective date of an appointment subject to investigation under § 731.301, OPM may instruct an agency to remove an appointee when it finds that the appointee is unsuitable for any of the reasons cited in § 731.202.

(b) Thereafter, OPM may require the removal of an employee on the basis of either intentional false statement or deception or fraud in examination or appointment; or refusal to furnish testimony; or statutory or regulatory bar.

(c) An action to remove an appointee or employee taken pursuant to an instruction by OPM is not an action under part 752, or §§ 315.804 through 315.806 of part 315, of this chapter.

(d) When OPM instructs an agency to remove an appointee or employee under this part it shall notify the agency and the appointee or employee of its decision in writing.

(e) Before OPM, or any agency having delegated authority from OPM under this part, shall take a final suitability action against an applicant, eligible, appointee, or employee under this part, the person against whom the action is proposed shall be given notice of the proposed action (including the availability for review, upon request, of the materials relied upon), an opportunity to answer, notice of the final decision on the action, and notice of rights of appeal, if any, all in accordance with this part.

§ 731.304 Debarment.

(a) When OPM finds a person unsuitable for any reason named in § 731.202, OPM, in its discretion, may deny that person examination for and appointment to a competitive position for a period of not more than 3 years from the date of determination of unsuitability.

(b) On expiration of a period of debarment, a person who has been debarred may not be appointed to any position in the competitive service until OPM has redetermined that person's suitability for appointment.

Subpart D—Suitability Actions

§ 731.401 Scope.

(a) *Coverage.* This subpart sets forth the procedures to be followed when OPM, acting under authority of this part, proposes to take or to instruct an agency to take, a final suitability ineligibility action, including removal, against an applicant or eligible for appointment in, or an appointee or employee in, the competitive service. This subpart does not apply to an action taken by an agency to which OPM has delegated authority under § 731.103.

(b) *Definition.* In this subpart, *days* means calendar days.

§ 731.402 Notice of proposed action.

(a) OPM shall notify the applicant, eligible, appointee, or employee (hereinafter, the "respondent") in writing of the proposed action and of the charges against the respondent. The notice shall state the reasons, specifically and in detail, for the proposed action. The notice shall also state that the respondent has the right to answer this notice in writing. If the respondent is an employee the notice shall further state that the employee may also make an oral answer, as specified in § 731.403(a). The notice shall further inform the respondent of the time limits for answer as well as the address to which such answer should be made.

(b) OPM shall send a copy of this notice to the agency, if any, that is involved. The notice shall be served upon the respondent by being mailed to the respondent's last known resi-

dence or duty station no less than 30 days prior to the effective date of the proposed adverse action. If the respondent is employed in the competitive service on the date the notice is served, the respondent shall be entitled to be retained in pay status during the notice period.

§ 731.403 Answer.

(a) *Respondent's answer.* A respondent may answer the charges in writing and furnish affidavits in support of the response. A respondent who is an employee may answer orally. The respondent may be represented by a representative of the respondent's choice, and such representative shall be designated in writing to OPM. To be timely, a written answer shall be made to OPM no more than 30 days after the date of the notice of proposed action. In the event that an employee requests to make an oral answer, OPM shall determine the time and place thereof. OPM shall consider any answer that the respondent makes in reaching a decision.

(b) *Agency's answer.* In actions proposed by OPM under 5 CFR 5.3, the agency may also answer the notice of proposed action. The time limit for filing an answer is 30 days from the date of the notice. OPM shall consider any answer that the agency makes in reaching a decision.

§ 731.404 Decision.

OPM shall notify the respondent and the agency of the decision. The decision shall be in writing, be dated, and inform the respondent of the reasons for the decision. Removal of appointees or employees will be effective 30 days following the date of the decision. The respondent shall also be informed that an adverse decision can be appealed in accordance with subpart E of this part.

Subpart E—Administrative Review and Appeal

§ 731.501 OPM Review Panel.

(a) *Composition.* The OPM Review Panel (the Panel) is composed of 3 members. The Director of OPM in his/her sole discretion shall appoint

the members of the Panel from among employees of OPM and shall designate one of them Chairman. The Chairman and members of the Panel shall be individuals who, by demonstrated ability, background, training, or experience in dealing with appellate matters or suitability issues are qualified to review OPM suitability determinations. This subpart does not apply to an action taken by an agency to which OPM has delegated authority under § 731.103, but agencies may establish similar procedures at their option.

(b) *Function.* The Panel's function is to review OPM determinations that an individual is unsuitable for employment in the competitive service and to affirm, reverse, or affirm as modified the OPM determination.

(c) *Decisions.* The Panel shall make the decision by majority vote.

§ 731.502 Procedures.

(a) *Time of filing.* When OPM issues a decision that an individual is unsuitable for employment, the individual may appeal the decision to the Panel within 30 days of the date of the decision.

(b) *Untimely filing.* If the 30-day time limit is not met the Panel will dismiss the appeal as untimely filed unless good cause for the untimely filing is demonstrated.

(c) *Computation of time.* In computing the number of days allowed for filing an appeal, the first day counted is that day after the date of the decision. If the date that would be the last day for filing falls on a Saturday, Sunday, or Federal holiday, the individual may file his/her appeal on the first workday after the date.

§ 731.503 Content of appeal.

(a) *Who may appeal.* Only an individual whom OPM has determined to be unsuitable for employment or his/her representative may file an appeal with the panel.

(b) *Content of appeal.* An appeal must include:

(1) The name, address, and telephone number of the appellant.

(2) A statement of the reasons why the appellant believes OPM's determination of unsuitability was incorrect together with any supporting docu-

mentation that he/she wishes the Panel to consider.

(c) *Service.* An appeal shall be served by personal delivery or by United States Mail to the Office of Personnel Management Suitability Review Panel, 1900 E Street, NW., room 800E, Washington, DC 20415, or P.O. Box 886, Washington, DC 20044. If the appeal concerns an individual employed at a Federal agency, the individual shall also serve a copy of the appeal upon the agency at which the action took place.

§ 731.504 Representation.

An individual may represent himself/herself or may designate a representative. An employing agency may disallow the choice of an individual as a representative that would result in a conflict of interest of position, that would conflict with the needs of the agency, or that would give rise to unreasonable costs to the Government. Before accepting a designation as representative, employees in the executive branch should consult 18 U.S.C. 205. An applicant may not be represented by an employee of an agency.

§ 731.505 Pay status.

When an employee or appointee whom OPM has determined to be unsuitable files an appeal the employing agency shall retain him or her in a pay status until the Panel issues its decision. If the Panel affirms OPM's decision, the employing agency shall remove the employee or appointee from the rolls within 5 days of receipt of the Panel's decision.

§ 731.506 Decision.

(a) After reviewing the record, the Panel shall prepare a written decision, affirming, reversing, or affirming as modified OPM's decision. The decision, if adverse, will inform the respondent of the right to appeal to the Merit Systems Protection Board under § 731.508 below.

(b) The Panel, in its discretion, may remand the case for additional investigation or consideration of relevant factors as it deems appropriate.

§ 731.507 Scope of review.

The Panel shall review de novo the OPM decision on the record. OPM bears the burden of proving by a preponderance of the record evidence that its decision would promote the efficiency of the service. If an issue of timeliness is raised, the individual appealing the OPM decision bears the burden of proving that his/her appeal was filed in a timely manner.

§ 731.508 Appeal to the Merit Systems Protection Board.

(a) *Appeal to the Merit Systems Protection Board.* An individual whom the Panel has decided is unsuitable for employment may appeal the Panel's decision to the Merit Systems Protection Board (the Board).

(b) *Exhaustion of remedies.* An individual may not appeal a determination of unsuitability to the Board unless he/she has perfected an appeal with the Panel and has received a decision from the Panel that he/she is unsuitable for Federal employment.

(c) *Appeal procedures.* The procedures for filing an appeal with the Board are found at part 1201 of title 5, Code of Federal Regulations.

Subpart F—Reemployment Eligibility

§ 731.601 Reemployment eligibility of certain former Federal employees.

(a) *Request for suitability determination.* When an employee has been removed by an agency on charges (other than security or loyalty) or has resigned on learning the agency planned to prefer charges, or while charges were pending, the former employee may request OPM to determine his or her suitability for further employment in the competitive service. OPM shall consider the request only if the former employee:

- (1) Has completed any required probationary period;
- (2) Has basic eligibility for reinstatement; and
- (3) Includes a sworn statement with the request which sets forth fully and in detail the facts surrounding the removal or resignation.

(b) *Action by OPM.* (1) OPM, after appropriate consideration, including

any investigation OPM deems necessary, shall inform the former employee of his or her current suitability for employment in the competitive service.

(2) If the former employee is found unsuitable and has had an opportunity to comment on the reasons for this finding, or has furnished comments to OPM, then OPM may cancel his or her reinstatement eligibility if that eligibility was obtained through fraud. In addition, OPM may prescribe a period of debarment from the competitive service not to exceed 3 years from the date of determination of unsuitability.

Subpart G—Savings Provision

§ 731.701 Savings provision.

No provision of these regulations shall be applied in such a way as to affect any administrative proceeding pending at the effective date of such provision. An administrative proceeding is deemed to be pending from the date of the "notice of proposed action" described in § 731.303 of this part.

PART 732—NATIONAL SECURITY POSITIONS

Subpart A—Scope

Sec.

732.101 Purpose.

732.102 Definition and applicability.

Subpart B—Designation and Investigative Requirements

732.201 Sensitivity level designations and investigative requirements.

732.202 Waivers and exceptions to investigative requirements.

732.203 Periodic reinvestigation requirements.

Subpart C—Due Process and Reporting

732.301 Due process.

732.302 Reporting to OPM.

Subpart D—Security and Related Determinations

732.401 Reemployment eligibility of certain former Federal employees.

AUTHORITY: 5 U.S.C. 3301, 3302, 7312; 50 U.S.C. 403; E.O. 10450, 3 CFR, 1949-1953 Comp., p. 936.

SOURCE: 56 FR 18654, Apr. 23, 1991, unless otherwise noted.

Subpart A—Scope

§ 732.101 Purpose.

This part sets forth certain requirements and procedures which each agency shall observe for determining national security positions pursuant to Executive Order 10450—Security Requirements for Government Employment (April 27, 1953), 18 FR 2489, 3 CFR 1949-1953 Comp., p. 936, as amended.

§ 732.102 Definition and applicability.

(a) For purposes of this part, the term “national security position” includes: (1) Those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) positions that require regular use of, or access to, classified information. Procedures and guidance provided in FPM chapter 732 and related issuances apply.

(b) The requirements of this part apply to competitive service positions, and to Senior Executive Service positions filled by career appointment, within the Executive Branch, and agencies may apply them to excepted service positions within the Executive Branch.

Subpart B—Designation and Investigative Requirements

§ 732.201 Sensitivity level designations and investigative requirements.

(a) For purposes of this part, the head of each agency shall designate, or cause to be designated, any position within the department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the na-

tional security as a sensitive position at one of three sensitivity levels: Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive.

(b) Investigative requirements for each sensitivity level are provided in FPM chapter 732.

§ 732.202 Waivers and exceptions to investigative requirements.

(a) *Waivers.*—(1) *General.* A waiver of the preappointment investigative requirement contained in section 3(b) of Executive Order 10450 for employment in a sensitive national security position may be made only for a limited period: (i) In case of emergency if the head of the department or agency concerned finds that such action is necessary in the national interest; and (ii) when such finding is made a part of the records of the department or agency.

(2) *Specific waiver requirements.* (i) The preappointment investigative requirement may not be waived for appointment to positions designated Special-Sensitive under this part.

(ii) For positions designated Critical-Sensitive under this part, the records of the department or agency required by § 732.202(a)(1) of this part shall show what decision was made on obtaining prewaiver checks, as follows: (A) The nature of the emergency precluded obtaining prewaiver checks; or (B) checks were initiated but not all responses were received within 5 days; or (C) checks made and favorably completed are listed.

(iii) The waiver restriction is optional for positions designated Noncritical-Sensitive under this part.

(iv) When waiver is authorized, the required investigation must be initiated within 14 days of placement of the individual in the position.

(b) *Exceptions to investigative requirements.* (1) Pursuant to section 3(a) of E.O. 10450, the following positions are exempt from the investigative requirements of E.O. 10450, providing that the employing agency conducts such checks as it deems appropriate to insure that the employment or retention of individuals in these positions is clearly consistent with the interests of the national security:

(i) Positions that are intermittent, seasonal, per diem, or temporary, not to exceed an aggregate of 180 days in either a single continuous appointment or series of appointments; or

(ii) Positions filled by aliens employed outside the United States.

(2) Other positions that OPM, in its discretion, deems appropriate may be made exempt based on a written request to OPM by the agency head in whose department or agency the positions are located.

§ 732.203 Periodic reinvestigation requirements.

The incumbent of each position designated Special-Sensitive or Critical-Sensitive under this part shall be subject to periodic reinvestigation of a scope prescribed by OPM 5 years after placement, and at least once each succeeding 5 years. The employing agency will use the results of such periodic reinvestigation to determine whether the continued employment of the individual in a sensitive position is clearly consistent with the interests of the national security.

Subpart C—Due Process and Reporting

§ 732.301 Due process.

When an agency makes an adjudicative decision under this part based on an OPM investigation, or when an agency, as a result of information in an OPM investigation, changes a tentative favorable placement or clearance decision to an unfavorable decision, the agency must:

(a) Insure that the records used in making the decision are accurate, relevant, timely, and complete to the extent reasonably necessary to assure fairness to the individual in any determination.

(b) Comply with all applicable administrative due process requirements, as provided by law, rule, or regulation.

(c) At a minimum, provide the individual concerned:

(1) Notice of the specific reason(s) for the decision; and

(2) An opportunity to respond; and

(3) Notice of appeal rights, if any.

(d) Consider all available information in reaching its final decision.

(e) Keep any record of the agency action required by OPM as published in the Federal Personnel Manual and related issuances.

§ 732.302 Reporting to OPM.

(a) In accordance with section 9(a) of E.O. 10450, each agency conducting an investigation under E.O. 10450 is required to notify OPM when the investigation is initiated.

(b) In accordance with section 14(c) of E.O. 10450, agencies shall report to OPM the action taken with respect to individuals investigated pursuant to E.O. 10450 as soon as possible and in no event later than 90 days after receipt of the final report of investigation.

Subpart D—Security and Related Determinations

§ 732.401 Reemployment eligibility of certain former Federal employees.

(a) *Request.* A former employee who was terminated, or who resigned while charges were pending, from a department or agency of the Government under a statute or executive order authorizing termination in the interest of national security or on grounds relating to loyalty, and authorizing OPM to determine the eligibility for employment in another department or agency of the Government, may request OPM in writing to determine whether the individual is eligible for employment in another department or agency of the Government.

(b) *Action by OPM.* (1) OPM shall determine, and will notify the former employee, after appropriate consideration of the case, including such investigation as it considers necessary, whether the individual may be employed in another department or agency of the Government.

(2) If a former Federal employee found ineligible under this section has had an opportunity to comment on the reasons for the action, or has furnished them to OPM or to the former employing agency, OPM may cancel the reinstatement eligibility if the eligibility resulted from the last Federal employment and was obtained through fraud, and OPM may prescribe a period of debarment not to

fidence and shall not allow access to, or allow information to be disclosed from a statement except to carry out the purpose of this part. An agency may not disclose information from a statement except as OPM or the agency head may determine for good cause shown.

§ 735.411 Effect of employees' statements on other requirements.

The statements of employment and financial interests and supplementary statements required of employees are in addition to, and not in substitution for, or in derogation of, any similar requirement imposed by law, order, or regulation. The submission of a statement or supplementary statement by an employee does not permit him or any other person to participate in a matter in which his or the other person's participation is prohibited by law, order, or regulation.

§ 735.412 Specific provisions of agency regulations for special Government employees.

(a) Agency regulations issued under this subpart for special Government employees, as a minimum, shall contain provisions covering the reporting requirements set forth in this section.

(b) Except as provided in paragraph (c) of this section, each agency head shall require each special Government employee to submit a statement of employment and financial interests which reports:

- (1) All other employment; and
- (2) The financial interests of the special Government employee which the agency determines are relevant in the light of the duties he is to perform.

(c) An agency head may waive the requirement in paragraph (b) of this section for the submission of a statement of employment and financial interests in the case of a special Government employee who is not a consultant or an expert when the agency finds that the duties of the position held by that special Government employee are of a nature and at such a level of responsibility that the submission of the statement by the incumbent is not necessary to protect the integrity of the Government. For the

purpose of this paragraph, "consultant" and "expert" have the meanings given those terms by Chapter 304 of the Federal Personnel Manual, but do not include:

- (1) A physician, dentist, or allied medical specialist whose services are procured to provide care and service to patients; or
- (2) A veterinarian whose services are procured to provide care and service to animals.

(3) A specialist appointed for intermittent confidential intelligence consultation of brief duration.

(d) A statement of employment and financial interest required to be submitted under this section shall be submitted not later than the time of employment of the special Government employee as provided in the agency regulations. Each special Government employee shall keep his statement current throughout his employment with the agency by the submission of supplementary statements.

[33 FR 12487, Sept. 4, 1968, as amended at 34 FR 6515, Apr. 16, 1969]

PART 736—PERSONNEL INVESTIGATIONS

Subpart A—Scope

- Sec.
- 736.101 Purpose and definitions.
 - 736.102 Notice to investigative sources.
 - 736.103 Protecting the identity of a source.
 - 736.104 Public availability of investigative files.

Subpart B—Investigative Requirements

- 736.201 Responsibilities of OPM and other Federal agencies.

AUTHORITY: Pub. L. 93-579; (5 U.S.C. 552a).

SOURCE: 56 FR 18655, Apr. 23, 1991, unless otherwise noted.

Subpart A—Scope

- § 736.101 Purpose and definitions.

(a) *Purpose.* The purpose of this part is to specify certain requirements for personnel investigations conducted by OPM, and for those conducted under delegated authority from OPM. The requirements of this part apply to

suitability and national security investigations conducted under parts 731 and 732 of this chapter; they also apply to investigations to determine eligibility or qualifications not covered in parts 731 and 732 of this chapter. The requirements of this part apply to employees in the civil service of the Executive Branch and to persons performing contract, voluntary or indirect services for the Federal Government, as set forth in subsection (b) below.

(b) *Definitions.* For the purposes of this part, (1) *Federal employment* includes the following range of services performed for the Federal government: (i) All employment in the competitive or excepted service or the Senior Executive Service in the Executive Branch; (ii) appointments, salaried or unsalaried, to Federal Advisory Committees or to membership agencies; (iii) cooperative work assignments in which the individual has access to Federal materials such as examination booklets, or performs service for, or under supervision of, a Federal agency while being paid by another organization such as a State or local government; (iv) volunteer arrangements in which the individual performs service for, or under the supervision of, a Federal agency; and (v) volunteer or other arrangements in which the individual represents the United States Government or any agency thereof.

(2) *Agency* means any authority of the Government of the United States, whether or not it is within or subject to review by another agency, and includes any executive department, military department, Government corporation, Government-controlled corporation, or other establishment in the executive branch of the Government, or any independent regulatory agency.

(3) *Personnel investigation* means an investigation conducted by written or telephone inquiries or through personal contacts to determine the suitability, eligibility, or qualifications of individuals for Federal employment, for work on Federal contracts, or for access to classified information or restricted areas.

§ 736.102 Notice to investigative sources.

(a) The agency investigator will notify the source from whom informa-

tion is requested, whether in person or by telephone, of the purpose for which the information is being sought and of the uses that may be made of the information. The interviewing agent must notify each person interviewed and each custodian of records contacted that all information provided, including the record source's identity, may be disclosed upon the request of the subject of the investigation.

(b) The interviewing agent may grant a pledge to keep confidential the identity of an information source upon specific request by the source. In addition, the agent has discretion to offer the source a pledge of confidentiality where the agent believes that such a pledge is necessary to obtain information pertinent to the investigation. A pledge of confidentiality may not be assumed by the source. The interviewing agent may not suggest to a source that the source request confidentiality.

(c) Where information is requested by written inquiry, the form, instructions, or correspondence used by an agency will include: (1) Notification that all information furnished by the source, including the source's identity, except for custodians of law enforcement or educational records, may be disclosed upon the request of the subject of the investigation; and (2) Space for the information source to request a pledge that the source's identity will not be disclosed to the subject of the investigation; or (3) An offer to make special arrangements to obtain significant information which the source feels unable to furnish without a promise that the source's identity will be kept confidential.

(d) A pledge of confidentiality, if granted, extends only to the identity of the source, and to any information furnished by the source that would reveal the identity of the source.

§ 736.103 Protecting the identity of a source.

When a source is granted a promise that the source's identity will be kept confidential, the investigative agency and all other agencies that receive information obtained under the promise

are required to take all reasonable precautions to protect the source's identity. Each agency will prepare for its investigators and agents implementing instructions consistent with this part.

§ 736.104 Public availability of investigative files.

(a) Investigative files are records subject to the Privacy Act and the Freedom of Information Act and are made available to requesters in accordance with the provisions of those Acts.

(b) Requests for investigative records are to be submitted to the Office of Personnel Management, Federal Investigations Processing Center, FOI/PA, Boyers, Pennsylvania 16018.

Subpart B—Investigative Requirements

§ 736.201 Responsibilities of OPM and other Federal agencies.

(a) Unless provided otherwise by law, the investigation of persons entering or employed in the competitive service, or by career appointment in the Senior Executive Service, is the responsibility of OPM.

(b) Requests for delegated investigating authority. Agencies may request delegated authority from OPM to conduct or contract out investigations of persons entering or employed in the competitive service or by career appointment in the Senior Executive Service. Such requests shall be made in writing by agency heads, or designees, and specify the reason(s) for the request.

(c) Timing of investigations. Investigations required for positions must be initiated within 14 days of placement in the position except for: Positions designated Critical-Sensitive under part 732 of this chapter must be completed preplacement, or post-placement with approval of a waiver in accordance with § 732.202(a) of this chapter; and for positions designated Special-Sensitive under part 732 of this chapter must be completed preplacement.

PART 752—ADVERSE ACTIONS

Subpart A—Principal Statutory Requirements for Suspension for 14 Days or Less

Sec.
752.101 Principal statutory requirements.

Subpart B—Regulatory Requirements for Suspension for 14 Days or Less

752.201 Coverage.
752.202 Standard for action.
752.203 Procedures.

Subpart C—Principal Statutory Requirements for Removal, Suspension for More Than 14 Days, Reduction in Grade or Pay, or Furlough for 30 Days or Less

752.301 Principal statutory requirements.

Subpart D—Regulatory Requirements for Removal, Suspension for More Than 14 Days, Reduction in Grade or Pay, or Furlough for 30 Days or Less

752.401 Coverage.
752.402 Definitions.
752.403 Standard for action.
752.404 Procedures.
752.405 Appeal and grievance rights.
752.406 Agency records.

Subpart E—Principal Statutory Requirements for Taking Adverse Actions Under the Senior Executive Service

752.501 Principal statutory requirements.

Subpart F—Regulatory Requirements for Taking Adverse Actions Under the Senior Executive Service

752.601 Coverage.
752.602 Definitions.
752.603 Standard for action.
752.604 Procedures.
752.605 Appeal rights.
752.606 Agency records.

AUTHORITY: 5 U.S.C. 7504 and 7514; 5 U.S.C. 1302, Pub. L. 96-494; Section 752.401 also issued under 5 U.S.C. 3301 and 3302, and E.O. 10577; Section 752.405 also issued under 5 U.S.C. 1302 and 7513; subpart F also issued under 5 U.S.C. 7543.

SOURCE: 45 FR 46778, July 11, 1980, unless otherwise noted.

**Sexual Orientation:
Security Criteria, Vulnerability and Secrets**

Tab F contains the following analytical material:

Enclosures

Subjects

- | | |
|---|---|
| 1 | A memorandum from Lorri L. Jean to the Board entitled "Adjudication Standards and Sexual Orientation." |
| 2 | A memorandum from Lorri L. Jean to the Board entitled "Personal Secrets and Vulnerability to Undue Influence: What is the Appropriate Analysis of Homosexual Conduct Kept Private?" |



Federal Emergency Management Agency

Region IX
Building 105
Presidio of San Francisco
San Francisco, CA 94129

August 6, 1992

MEMORANDUM FOR: FEMA SECURITY PRACTICES BOARD OF REVIEW
Lieutenant General Richard G. Trefry, Chair
General Andrew J. Goodpaster
Robert Kupperman
Julia Taft
Colonel Peter F. Dabrowski

FROM: Lorri L. Jean, Member 
FEMA Security Practices Board of Review

SUBJECT: Final Report: Adjudication Standards and Sexual Orientation

At the first meeting of the Security Practices Board of Review ("Board") on June 26, 1992, General Goodpaster raised a question concerning what pertinent authorities provide about the issue of homosexuality and security clearances. Specifically, after failing to find any mention of homosexuality in Executive Order 10450, the General inquired as to whether such authorities are concerned with "homosexuality per se, or attendant implications," such as being vulnerable to coercion. I volunteered to prepare a synopsis of the manner in which the pertinent authorities address the issue of sexual orientation in general, and homosexuality in particular.¹

¹ The terminology used to refer to sexuality in general and homosexuality in particular varies widely in the authorities examined in preparation for this synopsis. At times the language is clear and specific, and other times oblique. For purposes of this review, unless quoting directly from particular sources, the term "sexual orientation" will be used to refer generally to sexuality, e.g., heterosexuality and homosexuality. Sexual orientation is the proper term to use for several reasons. First, this is the term used by the definitive study on "Homosexuality and Personnel Security" prepared by the Defense Personnel Security Research and Education Center ("PERSEREC Study") in September, 1991. Second, it is the only term given legal validity in virtually every civil rights statute or ordinance nationwide protecting gay men and lesbians from discrimination, e.g., the District of Columbia Human Rights Act, the California Civil Code, the San Francisco Municipal Code, and the proposed Federal Civil Rights Act. Third, as the PERSEREC Study highlights, and as recent widely-reported medical studies appear to establish, an individual's heterosexuality or homosexuality does not result from simple "preference." Rather, adult sexual orientation has clear biological and sociological origins, and it cannot be changed by mere preference or whim.

For ease of reference, this memorandum highlights the manner in which the pertinent authorities do or do not address the issue of sexual orientation and/or homosexuality by citing excerpts of the actual language of those authorities. Portions of the text appearing in bold are those which currently or historically have been interpreted to apply to homosexuality.

Executive Order 10450: [Issued in 1953, this Order provides security requirements for government employment.] "[A]ll persons should receive fair, impartial, and equitable treatment at the hands of the Government...." See Preamble to the Order. Information developed in investigations conducted pursuant to this Order "shall relate, but shall not be limited, to the following: ... (iii) any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addition, **sexual perversion.**" See Section 8(a).

Executive Order 12356: [Issued in 1982, this order prescribes a uniform system for classifying, declassifying, and safeguarding national security information.] This Order contains no specific mention of sexual orientation in general, or homosexuality in particular. Rather, it simply provides that "A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes." See Section 4.1(a).

Department of Defense ("DoD") Adjudication Guidelines, CURRENT Version: Of the twelve factors examined in detail in Appendix I of the current guidelines, only the factor entitled "foreign connections/vulnerability to blackmail or coercion" specifically addresses sexual orientation, while meticulously avoiding the term "homosexuality." The discussion identifies as "disqualifying factors" any "Conduct or actions by the individual that increase the individual's vulnerability to possible coercion, blackmail or pressure ... including, but not limited to ... concealment or attempts to conceal from an employer ... **sexual preference, or sexual misconduct**" or "Concealment or attempts to conceal from immediate family members, or close associates, supervisors or coworkers ... **sexual preference or sexual misconduct.**" See DoD 5200.2-R, Appendix I, pp. I-13 and I-14. The possibly relevant "mitigating factors" for such "disqualifying information" are that the individual is willing to defend the United States against all threats and "is aware of the possible vulnerability to attempts of blackmail or coercion and has taken positive steps to reduce or eliminate such vulnerability." Id. at I-15.

The Adjudication Guidelines do not define the term sexual preference. The articulated basis for the "sexual misconduct" factor is as follows: "Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society." Id. at I-26. Neither perversion nor moral turpitude are specifically defined. However, the following conduct

is specified as behavior which would be a disqualifying factor: "Conduct determined to be criminal in the locale in which it occurred. Deviant or perverted sexual behavior which may include ... sodomy." Id. Neither "deviant or perverted sexual behavior" nor "sodomy" are defined.²

The discussion of the "sexual misconduct" factor reiterates as disqualifying conduct that which "increases the individual's vulnerability to blackmail, coercion or pressure," and describes one mitigating factor as a "Demonstration that the individual's sexual misconduct can no longer form the basis for vulnerability to blackmail, coercion or pressure." Id. at I-26 and I-27.

Department of Defense Adjudication Guidelines, PROPOSED DRAFT: On or about August of 1992, the DoD issued a draft of proposed revisions to DoD 5200.2R, entitled "Draft-2." This draft identifies the criteria for determining clearance eligibility under the security standards, and includes "Sexual acts, conduct or behavior that, because of the circumstances in which they occur, may indicate untrustworthiness, unreliability, lack of judgment, irresponsibility or vulnerability to blackmail or coercion." See DoD 5200.2R/Draft-2, Section 2-200q.³

² Interestingly, approximately half the states have no laws criminalizing sodomy. Further, in those that do, the definition of sodomy often includes oral (and/or anal) sexual contact between members of the same or opposite gender, including legally married spouses. This is the case with the sodomy statutes of Maryland, Virginia and the District of Columbia. See Maryland Ann. Code, Article 27, Section 554 (1991); Virginia Code Ann. Section 18.2-361 (1992); and 22 D.C. Code Section 3502 (1991). In the Security Practices Board of Review meeting on July 24, 1992, the DoD Deputy Director for Personnel Security, Peter R. Nelson, testified that the term "sodomy" in the current guidelines is "just a code word for homosexuality" and that it is being removed from the revised guidelines, just as the actual term "homosexual" was previously removed. See Official Transcript FEMA Security Practices Review Board, Friday, July 24, 1992, pp. 18-20. He also testified that the private commission of sodomy--whether heterosexual or homosexual--"is not normally an issue." Id. at 19. Rather, he stated that sodomy would only be an issue when a person "came to the attention of the criminal authorities ... for public acts, acts with a minor, ... for soliciting, things of that nature." Id. Mr. Nelson further stated that while sodomy (heterosexual or homosexual) may be a technical violation of state criminal law, it is generally impossible to prosecute, so DoD does "not generally consider [sodomy] a problem." Id.

³ The previous (current) version of the same provision read, "Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society." See DoD 5200.2R, Section 2-200q.

As in the current version, Appendix I of Draft-2 is a general discussion of adjudication policy designed "to assist DoD adjudicators in making personnel security determinations with respect to an individual's eligibility for assignment or retention in sensitive duties or eligibility for access to classified information." *Id.* at Appendix I, p. I-1. It also examines in detail twelve "Potentially Disqualifying Factors." In the factor entitled "foreign connections/vulnerability to blackmail or coercion," all explicit references to "sexual preference" or "concealment or attempts to conceal ... sexual preference" are deleted. *Id.* at I-24. However, the act of concealing or attempting to conceal "criminal conduct"⁴ from employers, family members, close associates, supervisors or co-workers is still deemed to increase an individual's vulnerability to coercion, blackmail or pressure. The mitigating factors remain essentially the same as those in the current version, cited above, except that the individual who is aware of the possible vulnerability must take positive steps to "significantly reduce or eliminate such vulnerability." *Id.* at I-25 (emphasis indicates added word).

The Appendix I of Draft-2 retains the disqualifying factor of "sexual misconduct," but changes the articulated basis for the factor to "Sexual acts, conduct or behavior that, because of the circumstances in which they occur, may indicate untrustworthiness, unreliability, lack of judgment, irresponsibility or vulnerability to blackmail or coercion." *Id.* at I-40. The proposed revision explicitly deletes the disqualifying factor of "Deviant or perverted sexual behavior which may indicate a mental or personality disorder (e.g., transsexualism, transvestism, exhibitionism, incest, child molestation, voyeurism, bestiality, or sodomy.)" *Id.* at I-41. However, it adds the following two provisions as disqualifying factors: "Sexual conduct that increases the individual's susceptibility to blackmail, pressure or coercion (e.g., transsexualism, transvestism, exhibitionism, homosexuality,⁵ ... or sodomy;" and "Sexual conduct that indicates poor judgment, unreliability or irresponsibility (e.g., ... sodomy). The retention of sodomy as a disqualifying factor appears to be contrary to the testimony before this Board that it was being removed from revised guidelines because DoD does not generally consider it to be a problem. See Footnote 2, *supra*.

⁴ As is mentioned in footnote 2, *supra*, half of the States criminalize sodomy, the definition of which encompasses much common heterosexual and homosexual conduct.

⁵ The Draft-2 revision appears to regress to the position of authorities which preceded the current version and which presumed without explanation, that homosexuality per se makes one vulnerable to coercion and/or blackmail. In fact, as noted above, the current version presumes only that concealment or attempt to conceal one's homosexuality renders one vulnerable to possible coercion and/or blackmail.

The possible mitigating factors retain the provision cited above, but add two provisions indicating that the potentially disqualifying sexual acts or conduct must not have involved force, violence, coercion or intimidation, and/or must have occurred in the past with no evidence of subsequent conduct of a similar nature. See DoD 5200.2R/Draft-2, Appendix I at I-42.

Department of Defense National Industrial Security Program ("NISP") Common Adjudicative Standards, PROPOSED DRAFT: As was indicated in testimony before the Board, the new draft of the common NISP adjudicative standards, issued on April 30, 1992, revises the relevant standards to include one called "sexual behavior." This standard contains no mention of sexual orientation or sodomy, but simply provides at page 7 that "Sexual behavior is a security concern only if it involves a criminal offense, indicates a personality disorder, exposes the individual to undue influence or coercion, or is blatant to the point that it reflects lack of judgment or discretion." The narrative goes on to state that "In the absence of specific security concerns, it is not an appropriate function of security clearance adjudicators to enforce codes of sexual behavior in the private lives of employees. Freedom of sexual expression is constitutionally protected if the behavior occurs in private and does not harm or exploit others."⁶ The discussion further provides that "there are a number of sexual behaviors that may signal a security concern: ... sexual behavior that causes an individual to be vulnerable to undue influence or coercion." However, no explanation is provided as to what sexual behaviors meet this standard. Finally, conditions that could reduce security concerns are identified as including when "the behavior no longer serves as a basis for undue influence or coercion." The proposed draft contains no other references pertinent to the issue of sexual orientation.

DoD Policy Memorandum, Subject: Eligibility of Homosexuals for DoD Security Clearances: This memorandum, issued on January 16, 1991, was written by Michael Sterlacci, DoD Assistant General Counsel, and widely distributed by Ray Pollari, Director of Counterintelligence and Investigative Programs. The Memorandum generally provides that an individual's homosexuality has a rational relationship to eligibility for security clearances if it makes the individual "susceptible to exploitation" or "reflects untrustworthiness, unreliability or lack of common sense judgment that must be demanded of anyone with access to classified

⁶ In August of 1992, an undated but allegedly more recent version of the draft NISP standards was received. This version was essentially the same as the April, 1992 version distributed for formal comment. Interestingly, however, the undated version does not include the preceding language about the impropriety of adjudicators enforcing codes of sexual behavior, or the language concerning freedom of sexual expression.

information." The Memorandum also essentially states that private sodomy between consenting adults, even if it violates state criminal laws, would not trigger the untrustworthiness, etc., standard articulated above.

DoD Answer to Noon Briefing Query, June 25, 1991: This document was issued by the Directorate for Defense Information, OSD News Division, in response to the following two queries: (1) Is there any evidence to suggest that gays are a greater security risk? (2) is it DoD policy that gays are security risks? The first query was answered in the negative. The answer to the second query stated that the significance of homosexuality must be determined on a case-by-case basis. The release identified as among the factors to be considered in determining whether homosexual behavior presents a security risk, whether "a particular individual ... engages in arts (sic) which are criminal, notorious, disgraceful, reckless or irresponsible, constitute sexual perversion, or indicate lack of judgment or stability. It is also relevant whether the particular conduct is criminal in the jurisdiction in which the subject resides, the extent to which the conduct occurs in public or private, is consensual, whether it involves minors, and whether it is indicative of instability or lack of good judgment, together with considerations of whether in the given case the individual is vulnerable to blackmail or otherwise may be coerced so as to act contrary to national interest." This articulation of policy appears not to be entirely consistent with the Pollari issuance five months earlier or with the NISP adjudicative standards.

Defense Investigative Service Manual for Personnel Security Investigations: The current (December, 1988) version of the manual used by Defensive Investigative Service ("DIS") investigators contains several sections entitled "Sexual Misconduct." One section provides that "sexual conduct can be a relevant consideration in circumstances in which deviant conduct indicates a personality disorder or could result in exposing the individual to direct or indirect blackmail or coercion. Such behavior includes homosexuality ... When expanding cases involving sexual misconduct and deviant activities, the Special Agent must determine the age of the person, voluntariness, the frequency of such activities, and the public nature and recency of the conduct, as well as any other circumstances which may serve to aggravate the nature or character of the conduct." See DIS 20-1-M, Section 4-10, p. 4-5.⁷

The second "Sexual Misconduct" section references Section 4-10 and prescribes procedures for interviews, stating that "because sexual behavior is generally considered a private and personal

⁷ This review analyzes only a few excerpts of the DIS manual (contained in Tab D(4) of the Security Practices Board of Review Reference Book), as DIS refused to permit access to a complete copy.

matter, utmost care must be taken in the preparation and the conduct of such sensitive and potentially controversial interviews. ... In view of the above Special Agents will not question Subject about sexual matters, unless Subject introduces the matter or it is developed through other sources." Id. at Section 5-44(a)(1), p. 5-57. This provision further cautions that "agents WILL NOT develop or report extensive, irrelevant details concerning the nature or type of sexual act engaged in; rather, a general categorization of the sexual act is sufficient (e.g., sodomy or sexual intercourse). ... It is not necessary to inquire about which partners were the passive/active partners." Id. at 5-44(a)(2)(a). The procedures require development of a profile of the subject's relationships. Id. at 5-44(a)(2)(b). They also require queries about aspects of the subject's "behavior and the partner's behavior that would increase Subject's vulnerability to blackmail, coercion or pressure." Id. at 5-44(a)(2)(c), p. 5-58. Such behavior is identified as including the following: "(5) Are Subject's family members, friends, and professional associates aware of Subject's activity? Has Subject failed to disclose his or her activity to any person referred to in the aforementioned question? Also determine if the partner's family, friends or professional associates are aware of the partner's activity? (6) Is there anyone from whom the Subject would conceal such activity? If the answer is affirmative, ascertain the identity of the person and the reason. (7) How would Subject respond if someone threatened to disclose Subject's activity to any members of Subject's family, or friends, professional associates, or the United States Government? Also determine how the partner would respond when confronted with such a situation." Id. at 5-44(a)(2)(c)(5), (6) and (7).

Finally, reporting requirements are prescribed mandating that specific information be included in the summaries of statements and/or interviews written by agents. Id. at 5-44(b), p. 5-59. With respect to alleged instances of "sexual misconduct," the mandated information includes: the nature, extent, and dates thereof; the "types of partners"; "the susceptibility to pressure, coercion, or blackmail"; "where the subject meets partners and where he engages in sexual misconduct"; whether the subject and/or partner(s) "are open about sexual misconduct"; future intentions; etc. Id. at 5-44(b)(3)(a)-(d), (f)-(h).

Stilwell Commission Report, "Keeping the Nation's Secrets": This report, issued in November of 1985, was provided to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices (the Commission was Chaired by General Richard G. Stilwell). The report focusses upon the protection of classified information, and contains numerous recommendations. The report contains no specific mention of sexual orientation or homosexuality, but does find that the adjudication process in which security clearance determinations are rendered must be improved. A primary basis for this finding is that decisions concerning eligibility for access to classified information "are made on the basis of vague criteria." See Executive Summary, Page 6. As this

synopsis establishes, the Stilwell Commission's criticism is perhaps most true in the context of adjudications involving sexual conduct.

Director of Central Intelligence Directive No. 1/14: [This Directive, most recently revised on January 22, 1992, concerns personnel security standards and procedures governing eligibility for access to Sensitive Compartmented Information ("SCI").] Annex A of this Directive provides the adjudication guidelines. Included therein is the statement that the ultimate determination to grant SCI access will be an "overall common sense determination" based on careful scrutiny of a variety of factors, including "sexual considerations." The descriptive narrative concerning "sexual considerations" notes that "sexual conduct is of legitimate concern to the SCI adjudicator where such conduct reflects a lack of judgment and discretion or when the conduct offers the potential for undue influence, duress, or exploitation." See DCID 1/14-11. The narrative then goes on to state, "Sexual behavior, including but not limited to deviant sexual behavior, can be a relevant consideration in circumstances in which it indicates flawed judgment, lack of discretion, irresponsibility, and/or a personality disorder, or could result in exposing the individual to direct or indirect pressure because of susceptibility to blackmail or coercion as a result of sexual behavior. Deviant sexual behavior includes, but is not limited to, bestiality, fetishism, exhibitionism, necrophilia, nymphomania or satyriasis, masochism, sadism, pedophilia, transvestism, and voyeurism."⁸ Whether under this new version of the DCID, or under the previous version (see footnote 8), it is commonly known that the Central Intelligence Agency ("CIA") denies security clearances (and thus employment, as all CIA positions are national security positions) on the basis of homosexual conduct per se. This has been conceded by the CIA in its briefs filed in the case of Webster v. Doe, 486 U.S. 592 (1988), which is on remand from the United States Supreme Court as Doe v. Gates. The Federal Bureau of Investigation has a similar per se exclusionary policy, as is clear from its recent answers to interrogatories in the case of Buttino v. FBI, Civil Action No.

⁸ It should be noted that Annex A in the previous version of DCID 1/14, dated April 14, 1986, contained the following explicit mention of homosexuality: "Homosexual conduct is also to be considered as a factor in determining an individual's judgment, discretion, stability and susceptibility to undue influence or duress." See Page PM 9-8d. This statement has been removed in the current version, as was the statement that "sexual promiscuity, prostitution, and extramarital relations are of legitimate concern to the SCI adjudicator where such conduct reflects a lack of judgment and discretion or when the conduct offers the potential for undue influence, duress or exploitation by a foreign intelligence service."

C-90-1639 (July 9, 1992), now before the United States District Court for the Northern District of California.

American Bar Association Model Security Clearance Standards: In the past year, the American Bar Association ("ABA") formally adopted a resolution calling for the establishment of published standards and procedures for the granting, denial, or revocation of security clearances (or eligibility for special access programs) for all employees of and applicants for employment by the federal government and its contractors, including DoD contractors. The ABA also has called for the establishment of a variety of due process procedures which include an opportunity for a hearing in revocation/denial cases pursuant to the Administrative Procedure Act.

The ABA also developed and recommended Federal adoption of a model security clearance standard based upon evaluation of eleven specific criteria. This recommendation stemmed primarily from the inconsistency the ABA found in the Federal sector's current security clearance adjudicative standards. Of the eleven criteria in the model standard, two may have particular relevance to the issue of homosexuality: the criminal conduct and sexual conduct criteria. The ABA "Criminal Conduct" criterion is written in a manner that appears to avoid the problem with sodomy statutes identified in testimony before the Board and discussed above. Specifically, the ABA narrative details the following disqualifying factors: conviction of or conduct which constitutes a felony under the United States Code⁹; conviction of a crime in which force, violence or intimidation was present, or which involved the use of dangerous weapons; conviction of a crime involving dishonesty, false statements, the abuse of an individual's spouse, or the abuse of children; etc.. See ABA Report on Recommended Uniform Standards for Access to Classified Information for Federal Government Employees and Employees of Federal Government Contractors, May 1991, pp. 10-12.

The ABA "Sexual Conduct" criterion states as its basis "sexual conduct which may lead the particular individual to submit to blackmail, coercion, or pressure for unauthorized disclosure of classified information is relevant to the granting or retention of a security clearance." *Id.* at 35. The disqualifying factor is identified as "sexual conduct which may lead the particular individual to submit to blackmail, coercion, or pressure for unauthorized disclosure of classified information." The discussion does not include whether or in what circumstances homosexuality is deemed to be conduct which may lead to the feared result.

Other Executive Department and Agency Standards: A review of several examples of adjudicative standards adopted by other non-DoD Executive Departments and Agencies has revealed that they generally replicate the DoD standards, but with numerous individual

⁹ The United States code contains no provisions criminalizing sodomy.

variances. Some are better drafted than the examples discussed above, and others use even more vague, undefined, intrusive and entirely subjective terminology. None appear to have seriously grappled with the issue of whether and/or when sexual conduct (heterosexual or homosexual) engaged in privately by consenting adults increases an individual's vulnerability to blackmail, coercion or pressure. Nor do any appear to question the implicit and explicit presumption of the DoD Policies and DCID 1/14 that gay and lesbian people who have not told the world of their sexual orientation, without more, are automatically vulnerable to blackmail, coercion or pressure.¹⁰

Two examples of other Agency standards include the United States Nuclear Regulatory Commission and Department of Energy ("DOE") adjudicative guidelines ("NRC"). The NRC guidelines were formally issued as regulations in November of 1988 (they appear at Title 10 of the Code of Federal Regulations, Chapter One). The DOE guidelines appear in an internal "working document" which is undated.

The NRC regulations make no mention of sexual conduct. Rather, the criteria for determining eligibility for access authorization and a security clearance include the following possibly pertinent examples: "has been convicted of crimes indicating habitual criminal tendencies," has a background where the conduct is "of a nature indicating poor judgment, unreliability or untrustworthiness," and has "engaged in any other conduct ... which tend[s] to show that the individual is not reliable or trustworthy, or which furnishes reason to believe that the individual may be subject to coercion, influence, or pressures which may cause the individual to act contrary to the national interest." See Section 10.11(a)(8), (9), and (13). No examples of conduct meeting such a standard are provided.

In the DOE guidelines, the criteria for determining clearance eligibility which could be deemed pertinent to the Board's inquiry are as follows:

* Mental or emotional disorders. "Conduct ... that ... reflect[s] abnormal behavior or instability even though there has been no history of mental illness or treatment, but which nevertheless may cause a defect in judgment or reliability." No definition of what constitutes abnormal behavior is provided.

* Honesty, reliability, trustworthiness, coercion, influence or pressure. "Has engaged in any unusual conduct or is subject to

¹⁰ An exhaustive search has failed to reveal any empirical or even anecdotal evidence which establishes any factual basis for this presumption. Rather, the presumption appears to be entirely speculative. As a result of some provocative comments made by members of this Board at the last meeting, it appears that an analysis of this issue would be helpful. Time permitting, such an analysis soon will be presented to the Board which evaluates the presumption and suggests a more consistent, relevant, equitable and humane approach to this issue.

any circumstances which tend to show that the individual is not honest, reliable, or trustworthy ... or which furnishes reason to believe that the individual may be subject to coercion, influence, or pressure which may cause the individual to act contrary to the best interest of the national security. Such conduct or circumstances include but are not limited to sexual activity ... or notoriously disgraceful conduct. ... In cases where the individual has committed felonious conduct but was not convicted of a felony, there are extenuating circumstances which mitigate the seriousness of the conduct such that it does not reflect a lack of trustworthiness or respect for the law. ... The disqualifying factors ... are ... criminal conduct involving commission of a state felony; ... criminal conduct punishable by confinement for one year or more; an established pattern of criminal conduct, whether the individual was convicted or not."

* Sexual misconduct. "Any acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment or lack of regard for the laws of society. ... The disqualifying factors ... are ... Deviant or perverted sexual behavior which may indicate a mental or personality disorder (e.g., ... sodomy). Spreading, or attempting to spread an infectious disease, such as AIDS, without informing the sexual partner" ... The conduct increases the individual's vulnerability to blackmail, coercion or pressure. ... The mitigating factors ... are ... Demonstration that the individual's sexual misconduct can no longer form the basis for vulnerability to blackmail, coercion or pressure."

* Vulnerability to blackmail or coercion. "The disqualifying factor ... is conduct or actions by the individual that increase the individual's vulnerability to possible coercion, blackmail or pressure ... including ... concealment or attempts to conceal from an employer ... sexual preference ... Concealment or attempts to conceal from immediate family members, or close associates, supervisors or coworkers ... sexual preference ... The mitigating factor, which may mitigate disqualifying information, is the individual is aware of the possible vulnerability to attempts of blackmail or coercion and has taken positive steps to reduce or eliminate such vulnerability."

FEMA Draft Standards: Tab L of the Board Reference Book contains a draft of FEMA's proposed "National Security Position Personnel Program" manual. In some instances, this manual appears to replicate the current DoD Adjudication Guidelines, and in other instances it appears to contain archaic and/or unique provisions.

" No other regulations, policy statements, directives, or guidance materials related to adjudicative standards were reviewed which make any reference to AIDS, particularly the "spreading" of the disease (whether with or without knowledge). This appears to be an example of the DOE Office of Safeguards and Security simply developing its own unique standard. Nothing indicates whether such a standard would be upheld if challenged legally.

Further, it appears to apply to all clearance adjudications those standards specified in the DCID No. 1/14 as governing only SCI access. Excerpts of possibly pertinent portions follow. "The criteria for determining eligibility for a clearance includes, but is not limited to, ... criminal or dishonest conduct; ... **sexual acts, conduct, or behavior** that, because of the circumstances in which they occur, may indicate untrustworthiness, unreliability, lack of judgment, irresponsibility, or vulnerability to blackmail or coercion." See Subsections 2-6 (g) and (p).

FEMA's draft manual also contains an Appendix which requires supervisors to report on-duty or off-duty conduct engaged in by employees when it falls in the following categories¹²: "Violation of any law ... and self-admitted criminal conduct ... Criminal conduct involving any sex practices or acts¹³; Adultery; ... Prostitution; ... Other sexual conduct including being a transvestite, sex changes, incest, sodomy and exhibiting in public." Id. at Appendix C, Section 3-c(14) and (22).

One of the more alarming provisions of the draft manual appears at Appendix D, which provides that "personnel security investigations will be considered devoid of significant adverse information unless they contain information listed below: ... All indications of moral turpitude, heterosexual promiscuity, **aberrant, deviant, or bizarre sexual conduct or behavior**, transvestitism, transsexualism, ... wife-swapping ... and similar situations from **whatever source.**" None of the highlighted terminology is defined. Nor is there any indication that this draft has received the approval of the FEMA Office of General Counsel. See Board Reference Book, Tab 8.

Federal Personnel Manual Chapter 731 - Personnel Suitability: [August 15, 1991 draft version; same as current version] While this Board has decided not to address suitability issues, a brief citation of the pertinent portions of the Federal Personnel Manual ("FPM") discussing suitability is useful. Only the "Suitability Adjudication" section addresses sexual conduct. The suitability

¹² No similar reporting requirements were discerned when perusing the authorities discussed herein. Thus, it appears that this section goes far beyond other standards. Further, it includes a requirement to report conduct which has been deleted from other authorities, and for which no relevance is shown. Some of the clearest of these examples are cited, regardless of whether they are relevant to the issue of sexual orientation.

¹³ As has been discussed in part above, such a provision would apply not only to sodomy, but to fornication (sexual intercourse by an unmarried person), which is criminalized by a number of jurisdictions, including Virginia. See Virginia Code Ann. Section 18.2-344 (1992).

referral chart requires referral for "rape, sexual assault, or other criminal misconduct." See FPM 731, Subchapter 4-1.¹⁴

FPM Chapter 732 - Personnel Security: [August 15, 1991 draft version; same as current version] The Subsection of this Chapter entitled "Security Adjudication" repeats the security criteria articulated in Executive Order 10450, e.g., "any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct ... or sexual perversion. ... Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause the person to act contrary to the best interests of the national security." See FPM 732, Subchapter 5-1. The remainder of this Chapter discusses various procedures, with no mention of anything particularly relevant to sexual orientation generally and/or homosexuality in particular.

FPM Chapter 736 - Personnel Investigations: [September 29, 1988 version] This chapter prescribes the procedures to be followed in both personnel suitability and security investigations. The only pertinent portion is subsection 2-5, "Restrictions in Conducting Personnel Investigations," which provides that "In conducting investigations, Federal personnel investigators are NOT authorized to ... interview applicants or appointees concerning their **sexual behavior or attitudes concerning sexual conduct** in the absence of allegations or information indicating **sexual misbehavior**, except when this information constitutes a bona fide qualification or fitness requirement for a specific position." No definition of "sexual misbehavior" is provided, nor are circumstances identified where such information constitutes a "bona fide qualification or fitness requirement" for a specific position.¹⁵

¹⁴ In 1976 and 1977, as a result of a number of court decisions, legislative enactments, and increased activity by the lesbian and gay civil rights movement, the Civil Service Commission amended its regulations so that no person could be denied Federal employment (i.e., deemed unsuitable therefore) solely on the basis of sexual orientation.

¹⁵ As with the FPM Chapters cited above, a draft version of FPM Chapter 736 was issued on August 15, 1991. This new version differs from the current version in several respects. In the following paragraph, language appearing in brackets appears in the current version but has been deleted from the draft version, and language appearing in bold does not appear in the current version but has been added in the draft version. All other language appears in both versions: "In conducting investigations, Federal personnel investigators are NOT authorized to ... interview applicants or appointees concerning their **sexual behavior or attitudes concerning sexual conduct** in the absence of allegations or information indicating sexual [mis]behavior which would have a bearing on efficient service in the position in question, or would

FPM Investigator's Handbook: [FPM Supp. (Int.) 736-71; October, 1991] The FPM Investigator's Handbook accompanying FPM Chapter 736 provides adjudicative guidance in addressing various issues during investigations. One section discusses how to handle the question of personal conduct by the subject of the investigation, in response to which issues of sexual behavior may arise. The handbook states that "homosexuality ... standing alone [does not constitute] a suitability issue, but, depending upon the type of case, could be either a security or public trust concern." See Page VII-16. The handbook further provides that during an investigation of a subject, when a source raises the issue of that subject's homosexuality, "follow-up questions as to whether such conduct is open or covert and whether the person could be subject to blackmail or coercion are necessary." *Id.* It also states that issues of a subject's homosexuality "should be reported as Issue Code 11 (issue related to loyalty and security) since it may be a concern when making a security determination. (See appendix C-11.)" *Id.* The Appendix C-11 provision referenced states that "homosexuality, in and of itself, while not a suitability issue, may be a security issue and must be addressed completely." *Id.* at C-8. No discussion is provided explaining what the phrase "addressed completely" means. Further, this handbook, on its face, applies to allegations raised during the investigation of a particular subject. It does not address the appropriate response to allegations of an individual's homosexuality arising outside the context or long after the completion of that individual's background investigation.

PERSEREC Study, "Homosexuality and Personnel Security," September, 1991: The PERSEREC Study is one of the few (and certainly the best) academic discussions of homosexuality and personnel security that has emanated from the Federal sector. While not every security professional or civil rights activist may agree with all that it contains, the PERSEREC Study includes thoughtful, even-handed, apparently objective analysis. In fact, the study contains such a wealth of information relevant to the work of this Board that it is commended to each of the Board members, to be read in its entirety. However, this brief synopsis will focus on the two questions which the PERSEREC Study explicitly addressed:

(1) Is a person a security risk by virtue of membership in the class homosexual? The Study's answer to this question is no, as "knowing that a person is homosexual tells very little about his or her character." See PERSEREC Study, p. 24.

interfere with or prevent effective performance by the employing agency of its duties and responsibilities [except when this information constitutes a bona fide qualification or fitness requirement for a specific position]." See FPM 736, Subchapter 2-5 (August 15, 1991 draft version). No explanation is provided concerning the circumstances in which sexual behavior would have a bearing on service or agency performance.

(2) Is a person of homosexual orientation a security risk because he or she is vulnerable to coercion and blackmail? The Study's answer to this question is more difficult to express in a single word. The Study addressed the issue of coercion and blackmail by discussing the concept of "personal secrets." Id. at 28-30. The most valuable and pertinent conclusion in this discussion was "If a homosexual person makes public, or is ready to make public, his or her sexual orientation, then vulnerability virtually disappears." Id. at 28. Another interesting conclusion was "Being homosexual no longer carries the automatic risk of vulnerability save in situations where it is expressly forbidden." Id. at 29. Yet, the Study itself concedes that there is no statistical evidence indicating that gay and lesbian people who view their sexual orientation as a "personal secret" have been vulnerable to coercion or blackmail even in situations where homosexuality is expressly forbidden. Id. at 29.¹⁶

Finally, the concluding paragraph of the PERSEREC Study is worth repeating:

The review and analysis of the literature on homosexuality leads to one conclusion: sexual orientation is unrelated to moral character. Both patriots and traitors are drawn from the class **American citizen** and not specifically from the class **heterosexual** or the class **homosexual**.

Id. at 32 (emphasis in original).

¹⁶ As mentioned previously, these issues will be analyzed more fully under separate cover. See footnote 10.



Federal Emergency Management Agency

Region IX
Building 105
Presidio of San Francisco
San Francisco, CA 94129

August 24, 1992

MEMORANDUM FOR: FEMA SECURITY PRACTICES BOARD OF REVIEW
Lieutenant General Richard G. Trefry, Chair
General Andrew J. Goodpaster
Robert Kupperman
Julia Taft
Colonel Peter F. Dabrowski

FROM: Lorri L. Jean, Member 
FEMA Security Practices Board of Review

SUBJECT: Final Report: Personal Secrets and Vulnerability
to Undue Influence: What is the Appropriate
Analysis of Homosexual Conduct Kept Private?

At the Federal Emergency Management Agency ("FEMA") Security Practices Review Board meeting on July 24, 1992, the Department of Defense ("DoD") Deputy Director for Personnel Security, Peter R. Nelson, presented a briefing on DoD Adjudication Standards. During his briefing, a lengthy discussion occurred concerning whether individuals who choose to keep their homosexuality private are deemed to be vulnerable to coercion and/or blackmail. Mr. Nelson stated that, generally, any person who chooses to keep his or her homosexuality a private matter, i.e., to remain in the closet, is deemed to be vulnerable to coercion and thus would be denied a clearance at the top secret and/or SCI level. See e.g., Official Transcript, FEMA Security Practices Review Board, Friday, July 24, 1992, pp. 17-18. Mr. Nelson indicated that such individuals would be denied top secret/SCI clearances even if they openly acknowledged their sexual orientation to security officials. Id. at 22. In fact, Mr. Nelson admitted that there had been cases in which individuals were forced to reveal their private heterosexual or homosexual behavior to others under threat of clearance denial. Id. at 23. Finally, it was conceded that such vulnerability is assumed even in the face of only six cases of espionage since the 1940's involving homosexuals, none of which involved coercion or blackmail on the basis of the individuals' sexual orientation. Id. at 45-47. A verbatim excerpt of the above colloquy appears at Appendix A.

This memorandum examines the current approach to evaluating the relevance, when determining eligibility for access to classified information at the top secret and/or SCI levels, of homosexual conduct which an individual chooses to keep private. It evaluates this approach within the larger context of personal secrets, and reaches the following conclusions:

* all people, including individuals cleared at the highest levels, have personal secrets they do not want revealed to all family members, employers, close associates and/or co-workers;

* personal secrets of equal relevance/irrelevance are not evaluated similarly when determining eligibility for access to classified information, e.g., individuals having the personal secret of homosexual conduct are treated more severely in the adjudication process than are individuals with equally relevant/irrelevant personal secrets;

* personal secrets should not be deemed to make individuals vulnerable to blackmail and/or coercion per se, and thus disqualify them for clearances at the top secret and/or SCI levels;

* the proper analysis for determining clearance eligibility is not merely discerning whether an individual has personal secrets, as every person does; rather, the relevant analysis which truly advances the interests of national security concerns both the nature of the personal secret (does it have any direct bearing on trustworthiness?) and whether any facts exist indicating that an individual would/would not be vulnerable to coercion and/or blackmail by a hostile intelligence agent threatening to expose the individual's personal secret;

* when analyzed properly, the personal secret of homosexual conduct has no direct bearing on trustworthiness, nor does it per se render an individual vulnerable to coercion and/or blackmail.

The basis for each of these conclusions is discussed in detail below.

Current Approach: Individuals who have kept their homosexual conduct a private matter are denied a clearance or forced to reveal their conduct to others to obtain a clearance.

As was indicated in the synopsis of adjudication standards and the issue of sexual orientation (presented to the Board on August 6, 1992), homosexuality is no longer viewed by DoD and most civilian departments and agencies as a per se basis for denial of a security clearance.¹ Rather, in the current version of the DoD Adjudication

¹ The two primary exceptions to this rule are the Federal Bureau of Investigation ("FBI") and the Central Intelligence Agency ("CIA"), both of which deny clearances (and thus employment) on the

Guidelines, the focus is upon whether an individual is vulnerable to coercion and/or blackmail. The guidelines identify as disqualifying factors any "Conduct or actions by the individual that increase the individual's vulnerability to possible coercion, blackmail or pressure ... including, but not limited to ... concealment or attempts to conceal from an employer ... sexual preference ... [and/or] concealment or attempts to conceal from immediate family members, or close associates, supervisors or coworkers ... sexual preference." See DoD 5200.2-R, Appendix I, p. I-14.

Thus, the DoD guidelines automatically assume, without explanation, that a person who desires to keep his or her homosexual orientation a private matter has increased his or her vulnerability to possible coercion, blackmail or pressure. Two identified circumstances which may mitigate such presumed disqualifying information are that the individual is willing to defend the United States against all threats, and that the individual is aware of the possible vulnerability to attempts to blackmail or coercion and has taken positive steps to reduce or eliminate such vulnerability. Id. at I-15. The appendix contains no description of what such positive steps might be. Clearly, according to the testimony before this Board, acknowledging one's sexual orientation to the security officials is not a sufficient positive step; rather, it appears that such private matters must be revealed to all family members, friends and co-workers in order to satisfy the mitigating factor standard. See July 24, 1992 Transcript, p. 23.

On April 30, 1992, DoD issued for comment a new set of Common Adjudicative Standards for the National Industrial Security Program. See Tab P of FEMA Security Practices Board of Review Reference Book. This new document proposes common adjudicative standards for determining eligibility for a security clearance or SCI access. Unlike the current guidelines discussed above, the proposed standards contain no mention of sexual orientation. Rather, the new standards focus on "sexual behavior," stating simply that sexual behavior is a security concern "only if it

basis of homosexual conduct per se. This has been conceded by the CIA in its briefs filed in the case of Webster v. Doe, 486 U.S. 592 (1988) (originally Doe v. Casey, now on remand as Doe v. Gates), and by the FBI in its recent answers to interrogatories in the case of Buttino v. FBI, Civil Action No. C-90-1639 (July 9, 1992), now before the United States District Court for the Northern District of California (the FBI appeared to rely upon semantics by claiming that it denied neither clearances nor employment on the basis of homosexual orientation, but conceded that it denied both from any individual engaging in homosexual conduct).

involves a criminal offense,² indicates a personality disorder, exposes the individual to undue influence or coercion, or is blatant to the point that it reflects lack of judgment or discretion." *Id.* at 7. The proposed standards go on to state that "In the absence of specific security concerns, it is not an appropriate function of security clearance adjudicators to enforce codes of sexual behavior in the private lives of employees. Freedom of sexual expression is constitutionally protected if the behavior occurs in private and does not harm or exploit others." *Id.* Conditions that "could reduce security concerns" are identified as "the behavior no longer serves as a basis for undue influence or coercion." *Id.* No further explanation is provided. Nor is it clear from the proposed standards whether an appendix will be included similar to that in the current guidelines (DoD 5200.2-R) which explicitly presumes that a person who desires to keep his or her homosexual orientation a private matter is vulnerable to undue influence or coercion. However, based upon the testimony presented to this Board, it appears that these disqualifying assumptions will continue to be applied. *See* July 24, 1992 Transcript, pp. 24-26.³

Flaws in the Current Approach: Inconsistent and misguided analysis of personal secrets generally does not advance the interests of national security.

This memorandum accepts as fact the conclusion of the Defense Personnel Security Research and Education Center study on "Homosexuality and Personnel Security" ("PERSEREC Study") that a person is not a security risk merely by virtue of homosexual orientation and/or engaging in homosexual conduct. *See* PERSEREC Study, September, 1991, p. 24. Indeed, as discussed previously, this conclusion appears to have been adopted in recent years by DoD and most civilian departments and agencies. The crucial question for examination, then, is the propriety of the current approach

² Unlike the current guidelines, the proposed standards drop any mention of sodomy, and thus appear to affirm the testimony before the Board that consensual sodomy is no longer considered by DoD to be a problem in clearance adjudications unless it "came to the attention of the criminal authorities ... for public acts, acts with a minor, ... for soliciting, things of that nature." *See* July 24, 1992 Transcript, p. 19. *But see* footnote 3, *infra*.

³ Subsequent to the first draft of this memorandum, DoD issued a draft of proposed revisions to 5200.2-R entitled "Draft-2." This new draft presumes not only that homosexual conduct kept private increases vulnerability to blackmail and/or coercion, but that homosexuality and/or sodomy *per se* increase such vulnerability. *See* DoD 5200.2-R/Draft-2, Appendix I at I-25 and I-41. This clearly is a regression from the current version of the guidelines and current practice.

used to evaluate whether someone who has engaged in homosexual conduct is a security risk, i.e., an approach which presumes that a person who desires to keep his or her homosexuality private is vulnerable to undue influence, coercion and/or blackmail. This section concludes that such a presumption is contrary to the evidence, and that DoD's current approach to analyzing personal secrets fails to advance the interests of national security.

Few adults today have managed to live lives that are paragons of virtue or innocence. It is reasonable to assert that all people have committed or continue to commit acts of which they are embarrassed. At the very least, everyone holds various matters private that they would not want revealed, depending upon the subject, to all family members, friends, co-workers, supervisors, or other people with whom they associate. Such "personal secrets" are maintained for a variety of reasons, ranging from fear of social ostracism to simple good taste. It is also reasonable to assert that occasionally a matter may be deemed so private by the individual secret-holder that he or she would do anything to avoid its disclosure, including revealing classified information to a hostile intelligence agent.

Logically, since everyone has personal secrets, the only 100% guaranteed way to ensure that no one with or seeking access to classified information is vulnerable to undue influence, coercion or blackmail as a result of a personal secret is for every single private fact of that person's life to be made public for all to know. Obviously, security professionals have never taken such an approach. First, it would be difficult to ensure that every single private fact of any individual's life was made public for all to know. Background investigations simply are not capable of gathering such information without relying fully on the subject's word. Second, the hue and cry from the millions of people who hold security clearances would shake the very foundations of our system of government. Third, there is no evidence whatsoever that the mere fact of holding a personal secret makes one vulnerable to undue influence, coercion and/or blackmail. The fact that it has never been standard practice in the security field to require exposure of all personal secrets of those seeking or holding clearances is proof of one of two things about personal secrets: either (1) they do not result in vulnerability per se; or (2) they DO result in vulnerability per se but the entire security field has negligently and incompetently failed to address this problem, thus endangering our national security. Obviously, the first conclusion is the only reasonable one.

Clearly, there has been an inconsistent approach in the security field with regard to personal secrets, both historically and in contemporary practice. For example, historically accepted (and contemporaneously known) facts of clandestine adulterous behavior by senior officials with the highest clearances in the land (including Presidents) were not dealt with as DoD's current

regulations and the testimony before this Board suggest. Such individuals were not forced to reveal their behavior to their spouses, families, co-workers, etc., to mitigate a supposed danger that they would be vulnerable. Nor is there any evidence that such individuals succumbed to coercion and/or blackmail. Thus, it can be convincingly argued that these examples alone establish that it is not the fact of a personal secret per se which determines that a person is vulnerable. Rather, the crucial inquiry is the nature of the personal secret in combination with whether the particular individual would compromise national security to protect it.

The legitimacy of this argument becomes eminently clear when one considers the manner in which various personal secrets are handled in the security clearance arena. Few personal secrets are treated as severely as homosexual conduct, i.e., resulting in clearance denial or a requirement to divulge the personal secret to all family members, co-workers, supervisors, friends, etc.. A non-exhaustive listing of examples of personal secrets⁴ is useful when considering this line of argument:

past marijuana use
 past drug or alcohol abuse
 serious drug abuse by one's children
 being born out of wedlock
 bearing or fathering children out of wedlock
 virginity, or lack thereof, when first married
 past victim of spousal abuse
 past victim of rape
 behavior in arguments with spouse
 being adopted
 having children who are adopted
 specific nature of sexual acts engaged in with spouse or date
 past divorce(s) and the reasons therefore
 masturbation practices now or as a child
 past abortion(s)
 abortion and/or pregnancy of unmarried daughter
 homosexual conduct as a youth
 fertility problems
 past adult or juvenile criminal record
 financial worth
 political party and/or voting record
 notorious parent or sibling
 number of sexual partners
 cosmetic surgery
 past victim of child abuse
 extramarital affairs

⁴ This listing is not intended to suggest that the matters described properly warrant shame or embarrassment. Rather, these are simply matters that many (and in some instances, most) people desire to keep private.

hair dye
 weight
 impotence
 family history of mental illness
 child's homosexuality
 past contraction of sexually transmitted disease
 HIV status
 toilet habits
 cancer or other serious health problems
 extramarital affairs of spouse

It is indisputable that a large percentage of people with clearances today have personal secrets which are mentioned above. It is equally indisputable that they likely would not want such secrets to be revealed to all of their friends, family, and co-workers, even though they might have shared certain personal secret(s) with some friends, family and/or co-workers (even security officials). Further, none of the personal secrets outlined above are per se determinative of trustworthiness. Nor can the concealment of (or attempt to conceal) such personal secrets from all or some of one's friends, family and/or co-workers reasonably be considered as always rendering one vulnerable to coercion and/or blackmail. Rather, the choice to keep such matters private and/or to determine which members (if any) of one's friends and family will be advised of such matters is an indelible part of each individual's right to privacy.

Similarly, there is no evidence in support of the assumption that individuals with such personal secrets, but no other indicia of lack of trustworthiness or vulnerabilities, would rather compromise the national security of the United States than have such secrets revealed, were such a threat made by a hostile intelligence agent. Individuals for whom homosexual conduct is a personal secret should be treated no differently.⁵ This is especially so in those cases

⁵ Occasionally, the personal secret of homosexual conduct or orientation is analogized to the personal secret of a clandestine extramarital affair. For example, this Board received testimony from a security professional stating that a homosexual who desired to keep his or her sexual orientation private "would be similar to a heterosexual who may be married and carrying on an illicit affair, does not want the spouse or family or colleagues to know about it. That certainly would bring to question the person's reliability or judgment and the possibility that the person could be exposed to some kind of pressure." See July 24, 1992 Transcript, p. 18.

Per se comparing homosexual conduct kept private to a clandestine extramarital affair is a false analogy. The most obvious example is two homosexual people in a monogamous, spousal-equivalent relationship, who desire to keep that relationship private from acquaintances in the workplace. It is clearly

where a homosexual person openly socializes with other lesbian and gay people but does not desire to share his or her sexual orientation with parents and/or everyone in the workplace. The key inquiry is not whether such an individual has disclosed his or her sexual orientation to the world, but whether the desire for privacy would outweigh the desire to protect the nation's secrets. Given that there have been no cases where closeted homosexual people have compromised the interests of national security because they were targets of blackmail,⁶ no factual basis exists to assume that

erroneous to equate such conduct with an "illicit" extramarital affair. In the latter case, the unfaithful spouse may face dissolution of his or her marriage and dire financial consequences if the infidelity is discovered. In the former case, no similar threat exists. Further, the latter case reasonably could be argued to have a direct impact upon trustworthiness, given that the individual is "cheating" on his or her spouse. In the former case, no such trustworthiness issue exists. Moreover, contrary to testimony cited above, there is no reasonable construction of the former case which would "certainly would bring to question the person's reliability or judgment."

Thus, except in those cases where the homosexual conduct kept private is also being hidden from an opposite-gender spouse, or a same-gender spousal-equivalent, it is inappropriate to compare it to an illicit extramarital affair. The respective behaviors have dissimilar relationships to trustworthiness, and dissimilar ramifications if revealed. Finally, as the historical cases referenced above indicate, even in the case of a clandestine, extramarital affair, it is questionable whether the person so engaged should per se be deemed likely to compromise national security to protect such a secret.

⁶ The PERSEREC data bank currently includes 117 cases of American citizens who between 1945 and the present committed or attempted to commit espionage. Only six of these individuals were identified as homosexual. However, their motives were the same as for heterosexuals: primarily money and secondarily, resentment. All were volunteers except one, who was recruited as an accomplice by a heterosexual friend. None was a target of blackmail. See PERSEREC Study, p. 30 (biographical sketches of the six known spies with a homosexual orientation appear at page 38).

This dearth of homosexual spies becomes even more telling when examined in light of the fact that for most of the years for which records were kept, and as of the dates that all but one of the spies were caught, civil rights for lesbian and gay people were virtually non-existent and vulnerability might have been more legitimately assumed. Yet, even in those days such vulnerability did not occur. Thus, in today's environment, where virtually every major city and numerous states in the United States (e.g., New York City, San Francisco, Washington, D.C., Chicago, Los Angeles, Hawaii, Connecticut, Massachusetts, Wisconsin) have laws protecting

closeted homosexuals, because of that fact alone, are vulnerable. Thus, per se rules to the contrary appear misguided.

As DoD's own PERSEREC study concluded, "If a homosexual person makes public, or is ready to make public, his or her sexual orientation, then vulnerability virtually disappears." See *id.* at 28. Interestingly, the PERSEREC Study highlights one example which proves this statement. The Study cites John Donnelly, Director of the Defense Investigative Service (1987), as reporting an anecdote in which foreign agents attempted to coerce into espionage a woman who was a closeted lesbian. The coercion involved disclosing her homosexuality. She refused to cooperate and reported the attempt to appropriate authorities, revealing her personal secret. *Id.* at 29. Thus, there is clearly more concrete evidence that closeted homosexuals are NOT vulnerable to undue influence, coercion and/or blackmail than there is that closeted homosexuals are so vulnerable. In light of such evidence, the only reasonable conclusion is that continued reliance upon the absolutely unsubstantiated vulnerability of individuals choosing to keep their homosexual orientations private emanates from, at least, archaic premises and ignorance or, at most, nefarious, discriminatory bias. In either event, such practices should not be permitted to continue, especially when they have no established relevance to advancing the interests of national security.

The Proper Approach: A consistent analysis of the relevance of personal secrets is in the Government's best interest as it protects national security while preserving individual privacy.

Pursuant to the above analysis, several conclusions are indisputable:

(1) all people have personal secrets they would not want revealed to all family members, friends and co-workers;

(2) the fact that people have personal secrets does not per se render them vulnerable to coercion and/or blackmail;

(3) the security field has not consistently addressed the issue of personal secrets, ignoring most personal secrets, and treating the personal secret of homosexual conduct more harshly than equally relevant or irrelevant personal secrets;

(4) no evidence exists that people who choose to keep their homosexual conduct private, whether entirely or only with regard to select family members, friends and/or co-workers, are more

gay and lesbian people from discrimination, it is even less likely that gay and lesbian people who have not told all of their family members and acquaintances of their sexual orientation would be vulnerable to blackmail if threatened with exposure.

vulnerable to coercion and/or blackmail as a result of maintaining such privacy; and

(5) the DoD unit established to specifically research personnel security matters has concluded people who have not revealed their homosexual conduct to the world are not vulnerable to coercion and/or blackmail so long as they "are ready to make public" such conduct.

As a result of these conclusions, it is apparent that the current practice of either denying security clearances to individuals who choose to keep their homosexual conduct private to any degree, or forcing them to reveal such conduct to all in order to obtain a clearance, is unnecessary and misguided. First, there is no evidence that this practice advances the interests of national security. Second, it is unnecessarily violative of such individuals' privacy (and, as one Board member suggested, it is extortionate, see July 24, 1992 Transcript at 23). Such intrusion is even less necessary in today's world, where the "threat" of hostile intelligence agents has been drastically reduced generally, let alone the unsubstantiated specific threat of such agents successfully targeting closeted homosexuals. Further, it is inconsistent for DoD to assert, on one hand, that "it is not an appropriate function of security clearance adjudicators to enforce codes of sexual behavior in the private lives of employees,"⁷ while requiring, on the other hand, that security clearance adjudicators enforce codes of communication between an employee and his or her family, co-workers and/or friends about the most private of matters, sexual behavior.

What is the proper role of security clearance professionals when it comes to the issue of personal secrets? As has been stated repeatedly above, personal secrets per se cannot possibly render an individual vulnerable to coercion and/or blackmail. Were that the case, almost no one would be suitable for security clearances. In fact, the logical, proper inquiry is: (1) do the individual's personal secrets have any direct relevance to trustworthiness?⁸ and (2) has anything been discovered in the individual's background investigation which legitimately indicates that he or she would sooner compromise the interests of national security than face revelation of his or her secret? With personal secrets where trustworthiness is not directly relevant, such as homosexual

⁷ See Proposed DoD Adjudication Guidelines, Tab P of FEMA Security Practices Board of Review Reference Book, at 7.

⁸ Examples of personal secrets which have direct relevance to trustworthiness include committing acts of embezzlement against a previous employer, income tax fraud, sexual abuse of a child and being expelled from an academic institution for cheating.

conduct kept private⁹, it should not be assumed that the personal secret increases the individual's vulnerability if information discussed in the second prong of the above inquiry has not been found. This is how other personal secrets with no direct relevance to trustworthiness have been treated in this past, and it is how all such secrets should be treated in the future.

Moreover, as in current practice, mitigating factors should be fairly considered. Both the current DoD guidelines and proposed standards state that one mitigating factor is when the behavior no longer serves as a basis for undue influence, blackmail or coercion. See Tab P of FEMA Security Practices board of Review Reference Book at 7 and DoD 5200.2-R, Appendix I, p. I-15. The current DoD guidelines further identify two relevant mitigating factors as (a) the individual is willing to defend the United States against all threats, and (b) the individual is aware of the possible vulnerability to attempts to blackmail and has taken positive steps to reduce or eliminate such vulnerability. See DoD 5200.2-R, Appendix I at I-15. Clearly, with regard to homosexual conduct kept private, the mitigating factors under both the current guidelines and proposed standards are satisfied. Under the proposed standards, because there is no evidence that such behavior serves as a basis for undue influence or coercion, the supposed security concern should be deemed reduced. Under the current guidelines, in the absence of evidence that the individual would not be ready to defend the United States, and in the face of no evidence that such behavior causes actual vulnerability, the fact of keeping the conduct private should not be considered disqualifying.

The logic of this approach becomes even more compelling in those situations where the individual honestly acknowledges his or her homosexual orientation and/or conduct to security professionals, even though he or she desires to keep such matters private from others. In such instances, neither the historical record nor logic warrant deeming such individuals to be vulnerable to coercion and/or blackmail. In the absence of additional information which factually establishes the individual's unreliability or lack of trustworthiness, there is no legitimate reason to believe that such individuals would compromise the interests of national security rather than reveal the private matter which they have already acknowledged to security officials. Rather, the more logical conclusion is that such individuals would be more likely to act as did the woman described in Director Donnelly's anecdote (who had not previously revealed her personal secret to security professionals): when faced with an instance of blackmail because of homosexual conduct kept private, they would refuse to cooperate

⁹ Excluding those rare instances when the homosexual conduct kept private is also being hidden from a spouse.

and would report the attempt to the appropriate authorities. See PERSEREC Study at 29.

RECOMMENDATIONS

It is clear from the above analysis that DoD's current approach to evaluating and "mitigating" homosexual conduct kept private is inappropriate. At most, DoD and FEMA (as well as other agencies implementing the DoD approach) should discontinue the current approach and adopt as a common adjudicative standard (with appropriate attendant guidance) the approach described above. At the very least, the FEMA Office of Security should update its approach to adjudicating homosexual conduct kept private in accordance with the approach outlined herein. Further, FEMA should amend the draft of its proposed Personnel Security Manual,¹⁰ to remove the outdated, undefined and unnecessary language highlighted in the August 6, 1992 memorandum concerning adjudication standards and sexual orientation.

¹⁰ See Tab L of FEMA Security Practices Board of Review Reference Book.

APPENDIX A

Excerpt from Official Transcript of
FEMA Security Practices Review Board
July 24, 1992

Colloquy between Peter R. Nelson, Deputy Director
for Personnel Security at the Department of Defense
and various members of the Board

MS. TAFT: You said that the whole point of [background investigations] is to ensure that a person is not subject to coercion, and you talked a lot about homosexuals who have come out of the closet. Do you make an assumption that if you refuse to come out of the closet or you're still in the closet that that can be equated with a tendency to be vulnerable to coercion?

MR. NELSON: I would say generally yes. It would be similar to a heterosexual who may be married and carrying on an illicit affair, does not want the spouse or family or colleagues to know about it. That certainly would bring to question the person's reliability or judgment and the possibility that the person would be exposed to some kind of pressure. It may be remote, especially if it is in the United States versus overseas, but the general rule is if the issue is homosexuality, the person says no, my friends don't know, I don't want my mother to know or my father or my colleagues, then I would say in that circumstance, generally a negative outcome would be forthcoming.

See Official Transcript, FEMA Security Practices Review Board, Friday, July 24, 1992, pp. 17-18.

MS. TAFT: I would like to get back to this closet case problem. If somebody, in the course of their security interview probably, admits confidentially that they are a lesbian or a homosexual, but doesn't want anybody else to know about it, is that still a closet case or is it not a closet case?

MR. NELSON: I would say it's still a closet case because that file is protected under the Privacy Act. The subject can get his or her investigative file with the exception of any other sources that may have requested confidentiality. So, we safeguard that information, protect it very, very tightly. No one else, other than the repository that holds the file, has access to that or your government adjudicators.

MS. TAFT: But it seems to me if somebody would come and be very honest about the fact, look, I have this proclivity or this side of my life, I don't want my wife to know about it or my husband to know about it, but I'm letting you know about it so that if anybody tries to

affect my employment, you know that I'm being honest with you. I guess that assumes that they aren't going to go to the wife or threaten to go to the wife or the husband.

MR. NELSON: You're putting me right on the spot, which I guess is what you intended, but it's a good question. Right now I can't say 100 percent of the time, and that's one of the issues we have. ... But in that case, I'm going to have to be honest. Right now the view would be we would have to look at that very, very carefully. The propensity would be again for a negative outcome. ...

DR. KUPPERMAN: Would you go so far as to tell someone that their clearances are going to be denied unless they reveal either their heterosexual or homosexual behavior?

MR. NELSON: That has occurred. That has happened.

DR. KUPPERMAN: It's a kind of extortion on our side.

Id. at pp. 21-23.

MS. JEAN: [Pete,] as long as we are putting you on the spot, as you called it, let me go a little bit more specifically into some of these questions.

If you had a person, let's say, who came to you and said, oh yes, I'm a lesbian and a number of my friends know, but I really don't make that an issue at work. I don't believe it's appropriate for the work place, and I've not told my parents because you don't discuss your sexual activities with your parents. I don't discuss them with mine. I'd prefer not to bother them with this. Of course, if someone ever came to me and threatened me, I would immediately come to you and would deal with my parents at that point, but I see no reason to do it now. That would not be good enough. You would say to remove this possible cloud, as you discussed it, you must tell your parents.

MR. NELSON: Well, again, I think like I indicated, it could depend on the type of access.

MS. JEAN: Let's say it's not a low level access.

MR. NELSON: I would say that if we are talking about top secret or SCI, it would be very probable that we would want the appropriate people to know, as far as the immediate family or colleagues. ...

But I would say it could depend on the circumstance, and that is why we have human beings adjudicating. Every case is different, has a little different spin or twist. As I say, other kinds of issues may come up. As we say, we try to look at the whole person. That sounds like a trite phrase, but I think it's true. That would be considered in the context not only of the other activities or the other facts in the

investigation, but also the kinds of accesses the person might have.

But as a general rule, as I say, as the practice has evolved and the way it is basically implemented today is are the people that are close to this person aware of their situation such that the possibility of coercion or pressure, if not eliminated, is mitigated.

Id. at pp. 24-26.

MS. JEAN: I just had one more question. You were throwing around these numbers about numbers of clearances in the millions, and I assume that since World War II, you have probably had tens of millions of people cleared.

I'm curious because in my research I have been unable to find any reference to any case. How many cases are you aware of--let's pick the last 40 years--where someone has breached national security as a result of being coerced or influenced because of their homosexual orientation?

MR. NELSON: There are some.

MS. TAFT: Six it says in there [referring to the report by the Defense Personnel Security Research and Education Center on "Homosexuality and Personnel Security"].

MR. NELSON: That's right out of our report.

MS. TAFT: Six out of 117.

MR. NELSON: As a matter of fact, we have--I am pretty sure I can make this available to you. It is another PERSEREC report. It's the unclassified espionage database. Back in the 1950's--and I can't think of the names--there were a couple of cases with NSA. Of course, some of the British cases.

DR. KAMENY: Those were not pressure or coercion. There were non since 1912 in Austria-Hungary.

COLONEL DABROWSKI: They were homosexuals, but they were not blackmailed or coerced.

DR. KAMENY: Exactly.

MR. NELSON: Right. I'm sure exactly which cases those were. ...

As we have said in some of our public releases, sexual conduct is just one of many areas that we're interested in as far as a potential weakness. In our view, if we ignore these, there is always that one chance, if it hasn't, indeed, occurred where it was a direct cause and effect, it could still.

But we do have some cases, most of which I think are classified, that we I'm sure could share with you on a classified basis where their homosexuality was, indeed, a factor. It may not have been a direct causative factor, but it was involved.

COLONEL DABROWSKI: Isn't another reason because you found that some of the enemy intelligence instructions that you were able to get hold of did mention certain sexual or people who were closet homosexuals as people that could be targeted?

DR. KUPPERMAN: Yes, but how that the sexual mores and standards are changing, it just becomes irrelevant.

GENERAL TREFRY: But you see, you pursue this. At the same time they might have targeted homosexuals, they also targeted other people, femme fatales--

MR. NELSON: Sure, oh, absolutely. In fact, there are obviously far more cases where there was a heterosexual inducement. There is no question about that. That's certainly of concern.

It's just that we're saying we can't afford to ignore any possibility because the consequences could be dire.

GENERAL TREFRY: Well, that's right, but Pearl Harbor has been a very expensive experience for the United States I can tell you that. We're going to make sure that never happens again. So, we have millions of clearances, you see, and thousands of people on alert 24 hours a day.

DR. KUPPERMAN: Which equates to no one being on alert.

GENERAL TREFRY: That's right.

Id. at pp. 45-48.

**DoD/NISP Criteria:
Sexual Conduct/Vulnerability**

Tab G contains the following analytical material:

Enclosures

Subjects

- | | |
|---|--|
| 1 | A side-by-side comparison of current (1987) and/or proposed (1990, 1992) security criteria for the Department of Defense (DoD) civilians and the National Industrial Security Program (NISP) civilian contractors concerning "sexual misconduct" or "sexual behavior." |
| 2 | A side-by-side comparison of current (1987) and/or proposed (1990, 1992) security criteria for DoD civilians and NISP contractors concerning foreign connections and vulnerability. |

The Board has included Enclosures 1 and 2 to supplement the analyses contained in Tab F and to highlight the most relevant security criteria that have and will continue to have the most significant influence on the current and future personnel security practices at FEMA with respect to homosexuals.

The Board also observes that these particular criteria, in their present form, allow security personnel to require applicants for security clearances to reveal their homosexuality to family members, employers and friends in order to mitigate or eliminate a perceived vulnerability to undue influence or coercion and thereby permit the granting of a security clearance.

The Board notes that the most recent DoD and NISP criteria allow or encourage practices that are contrary to the Board's recommendation on page 15 of the basic report which states:

"The Board recommends that federal regulations, standards, guidelines and other personnel security directives be revised to make it inappropriate and unnecessary, in the absence of

any other security concerns, for government security personnel to require any federal civilian employee or potential civilian employee to publicize his/her sexual orientation or that of any other person as a condition of employment or for obtaining a Federal Government security clearance.”

The Board also notes the DoD criteria in the April 1990 Draft of 5200.2-R explicitly promote the requirement for homosexuals to publicize their own sexual orientation, or that of others, because of the potential for blackmail or coercion. The August 1992 NISP guidelines, on the other hand, do not expressly mention homosexuals as possible targets for coercion or blackmail, but they are broad enough to permit individual agencies to require homosexuals to publicize their sexual orientation due to the possibility of blackmail or coercion.

Department of Defense (DoD), Personnel Security Program
DoD 5200.2-R Appendix I
(Adjudication Guidelines)

FOREIGN CONNECTIONS/VULNERABILITY . . .

Current Version
(1987)

Qualifying Factors

Behavior falls within one or more of the following categories):

. . .

Conduct or actions by the individual that increase the individual's vulnerability to possible coercion, blackmail or pressure, regardless of the country in which it occurred, including, but not limited to the following:

Concealment or attempts to conceal from an employer . . . sexual preference, sexual misconduct described under that section below. . . .

Concealment or attempts to conceal from immediate family members, or close associates, supervisors or coworkers . . . sexual preference, or sexual misconduct described under that section below.

Mitigating Factors

Circumstances which may mitigate the qualifying information):

Concerning the individual:

. . .

The individual is aware of the possible vulnerability to attempts of blackmail or coercion and has taken positive steps to reduce or eliminate such vulnerability.

Proposed Revision (Draft-2)
(April 1990)

Potentially Disqualifying Factors

(behavior may include, but is not limited to one or more of the following):

. . .

5. Conduct or actions by the individual that increase the individual's vulnerability to possible coercion, blackmail or pressure, regardless of the country (U.S. or foreign) in which it occurred, including, but not limited to the following:

a. Concealment of attempts to conceal from an employer . . . ~~sexual preference, or sexual misconduct described under that section below.~~ . . . (proposed deletions shown)

b. Concealment or attempts to conceal from immediate family members, close associates, supervisors or co-workers . . . ~~drug or alcohol abuse, sexual preference, or sexual misconduct described under that section below.~~ (proposed deletions shown)

Mitigating Factors

(circumstances that may mitigate potentially disqualifying behavior):

1. The individual:

. . .

j. The individual is aware of the possible vulnerability to attempts of blackmail or coercion and has taken positive steps to significantly reduce or eliminate such vulnerability.

National Industrial Security Program (NISP) Guidelines
Annex A
(Common Adjudicative Standards for Determining Eligibility for a Security Clearance or SCI Access)

FOREIGN INFLUENCE

Draft
(April 1992)

Conditions that may indicate undue foreign influence include:

. . .

(2) unreported association with nationals from countries or areas on this list (most recent official list of designated countries);

. . .

(4) conduct in a foreign country which makes the individual vulnerable to coercion, blackmail, or pressure by a foreign government;

. . .

Conditions that may reduce security concerns include:

(1) Contacts with foreign citizens are casual and have no relation to security risk;

. . .

(4) the individual's personal or financial interest in the United States appears sufficient to counter any potential pressure that might be brought to bear.

Draft
(August 1992)

Conditions that are of a security concern include:

. . .

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

. . .

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

. . .

Conditions that could reduce security concerns include:

(1) a determination that the immediate family member(s), cohabitant, or associate(s) in question would not constitute an unacceptable security risk;

. . .

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

Department of Defense (DoD), Personnel Security Program
DoD 5200.2-R, Appendix I
(Adjudication Guidelines)

SEXUAL MISCONDUCT

Current Version
(1987)

Disqualifying Factors

Behavior falls within one or more of the following categories:

The conduct involves:

...

j. Deviant or perverted sexual behavior which may indicate a mental or personality disorder (e.g., transsexualism, transvestism, exhibitionism, incest, child molestation, voyeurism, bestiality, or sodomy).

...

Mitigating Factors

Circumstances which may mitigate disqualifying information):

...

Demonstration that the individual's sexual conduct can no longer form the basis for vulnerability to blackmail, coercion or pressure.

Proposed Revision (Draft-2)
(April 1990)

Potentially Disqualifying Factors

(behavior which gives rise to the above mentioned security concerns ["... vulnerability to blackmail or coercion."], may include, but is not limited to one or more of the following):

...

8. Sexual conduct that increases the individual's susceptibility to blackmail, pressure or coercion (e.g., transsexualism, transvestism, exhibitionism, homosexuality, incest, child molestation, voyeurism, bestiality, or sodomy).

9. Sexual conduct that indicates poor judgment, unreliability or irresponsibility (e.g., transvestism, exhibitionism, incest, child molestation, voyeurism, bestiality, or sodomy).

Mitigating Factors

(circumstances that may mitigate potentially disqualifying behavior):

...

4. Demonstration that the individual's sexual misconduct can no longer form the basis for vulnerability to blackmail, pressure or coercion.

...

National Industrial Security Program (NISP) Guidelines
Annex A
(Common Adjudicative Standards for Determining Eligibility for a Security Clearance or SCI Access)

SEXUAL BEHAVIOR

Draft
(April 1992)

Sexual behavior is a security concern only if it involves a criminal offense, indicates a personality disorder, exposes the individual to undue influence or coercion, or is blatant to the point that it reflects lack of judgment or discretion.

In the absence of specific security concerns, it is not an appropriate function of security clearance adjudicators to enforce codes of sexual behavior in the private lives of employees. Freedom of sexual expression is constitutionally protected if the behavior occurs in private and does not harm or exploit others.

There are a number of sexual behaviors that may signal a security concern:

(3) sexual behavior that causes an individual to be vulnerable to undue influence or coercion;

Conditions that could reduce security concerns include:

(4) the behavior no longer serves as a basis for undue influence or coercion.

Draft
(August 1992)

Sexual behavior is a security concern if it involves a criminal offense, indicates a personality disorder, subjects the individual to undue influence or coercion, or reflects lack of judgement or discretion.

Conditions which signal security concern include:

(3) sexual behavior that causes an individual to be vulnerable to undue influence or coercion;

Conditions that could reduce security concerns include:

(4) the behavior no longer serves as a basis for undue influence or coercion;