DOD 5200.2-R

DEPARTMENT OF DEFENSE

PERSONNEL SECURITY PROGRAM

JANUARY 1987

ADMINISTRATIVE REISSUANCE INCORPORATING
THROUGH CHANGE 3, FEBRUARY 23, 1996

OFFICE OF THE DEPUTY UNDER SECRETARY OF DEFENSE
(POLICY)

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

POLICY

December 16, 1986

FOREWORD

This "Personnel Security Program Regulation" is reissued under the authority of DoD Directive 5200.2, "DoD Personnel Security Program," December 20, 1979. It contains expanded direction and procedures for implementing those references cited in Chapter 1 and in Appendix A of this Regulation that pertain to acceptance and retention of DoD military, civilian, consultant and contractor personnel and of granting such persons access to classified information or assignment to a sensitive position. It also implements such recommendations from the Defense Security Review Commission Report as pertains to personnel security and approved by the Secretary of Defense.

DoD 5200.2-R, "Department of Defense Personnel Security Program," December 1979, is hereby canceled as of December 31, 1986. The effective date of this Regulation is January 1, 1987.

The provisions of this Regulation apply to the Office of the Secretary of Defense (OSD) and activities supported administratively by OSD, the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies.

This Regulation is mandatory for use by all DoD Components. Heads of DoD Components may issue supplementary instructions when necessary to provide for internal administration of this Regulation within their respective components.

Forward communications, including recommended changes, regarding this Regulation and copies of supplemental instructions issued, through appropriate channels to: Deputy Under Secretary of Defense for Policy, Attention: Director Counterintelligence and Investigative Programs, Room 3C-267, The Pentagon, Washington, D.C. 20301-2200.

This Regulation is being published in Title 32, Code of Federal Regulations (CFR). DoD Components may obtain copies of this Regulation through their own publications channels. Federal Agencies and the public may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

Craig Alderman, Jr.
Deputy

TABLE OF CONTENTS

	Page
FOREWORD	2
TABLE OF CONTENTS	3
REFERENCES	5
DEFINITIONS	8
CHAPTER 1 - GENERAL PROVISIONS	13
C1.1. - PURPOSE AND APPLICABILITY	13
CHAPTER 2 - POLICIES	15
C2.1. - STANDARDS FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES	15
C2.2. - CRITERIA FOR APPLICATION OF SECURITY STANDARDS	15
C2.3. - TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS	18
C2.4. - AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES	22
C2.5. - LIMITATIONS AND RESTRICTIONS	26
CHAPTER 3 - PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS	29
C3.1. - SENSITIVE POSITIONS	29
C3.2. - CIVILIAN EMPLOYMENT	31
C3.3. - MILITARY APPOINTMENT, ENLISTMENT, AND INDUCTION	33
C3.4. - SECURITY CLEARANCE	34
C3.5. - SPECIAL ACCESS PROGRAMS	46
C3.6. - CERTAIN POSITIONS NOT NECESSARILY REQUIRING ACCESS TO CLASSIFIED INFORMATION	52
C3.7. - REINVESTIGATION	56
C3.8. - AUTHORITY TO WAIVE INVESTIGATIVE REQUIREMENTS	59
CHAPTER 4 - RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATION AND PERSONNEL SECURITY DETERMINATIONS	60
CHAPTER 5 - REQUESTING PERSONNEL SECURITY INVESTIGATIONS	63
CHAPTER 6 - ADJUDICATION	66
CHAPTER 7 - ISSUING CLEARANCE AND GRANTING ACCESS	70
CHAPTER 8 - UNFAVORABLE ADMINISTRATIVE ACTIONS	73
C8.1. - REQUIREMENTS	73
C8.2. - PROCEDURES	76
C8.3. - REINSTATEMENT OF CIVILIAN EMPLOYEES	78

CHAPTER 9 - CONTINUING SECURITY 80
C9.1. - EVALUATING CONTINUED SECURITY ELEGIBILITY 80
C9.2. - SECURITY EDUCATION 82

CHAPTER 10 - SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS 86

CHAPTER 11- PROGRAM MANAGEMENT 89

CHAPTER 12 - DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII) 92

APPENDICES

APPENDIX 1 - INVESTIGATIVE SCOPE 97

APPENDIX 2 - REQUEST PROCEDURES 111

APPENDIX 3 - TABLES FOR REQUESTING INVESTIGATIONS 117

APPENDIX 4 - REPORTING OF NONDEROGATORY CASES 124

APPENDIX 5 - DOD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES 125

APPENDIX 6 - GUIDELINES FOR CONDUCTING PRE-NOMINATION PERSONAL INTERVIEWS 129

APPENDIX 7 - (LEFT BLANK FOR FUTURE USE) 131

APPENDIX 8 - ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION 132

APPENDIX 9 - OVERSEAS INVESTIGATIONS 153

APPENDIX 10 - ADP POSITION CATEGORIES AND CRITERIA FOR DESIGNATING POSITIONS 162

APPENDIX 11 - SAMPLE NOTIFICATIONS FOR ADVERSE PERSONNEL SECURITY DETERMINATIONS 164

APPENDIX 12 - STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD 183

APPENDIX 13 - CONDUCT OF A PERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE (AJ) 185

REFERENCES

(a) DoD 5200.2-R, "DoD Personnel Security Program," January 1987, authorized by DoD Directive 5200.2, May 6, 1992

(b) DoD 5220.22-R, "Industrial Security Regulation," authorized by DoD Directive 5220.22, December 8, 1980

(c) DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," February 2, 1992

(d) Reference Not Used

(e) Public Law 88-290, "National Security Agency - Personnel Security Procedures," March 26, 1964 (78 STAT. 168)

(f) Public Law 86-36, "National Security Agency Officers and Employees," May 29, 1959 (73 Stat. 63)

(g) Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953

(h) Executive Order 12333, "United States Intelligence Activities," December 4, 1981

(i) DoD Directive 5210.45, "Personnel Security in the National Security Agency," May 9,1964

(j) Executive Order 1295.8, "Classified National Security Information," April 17,1995

(k) Executive Order 11935, "Citizenship Requirements for Federal Employment," September 2, 1976

(l) Director of Central Intelligence Directive (DCID) No. 1/14, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," January 22, 1992

(m) Section 552a of title 5, United States Code

(n) DoD Directive 5100.23, "Administrative Arrangements for the National Security Agency, May 17, 1967

(o) Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979

(p) DoD Directive 5210.48, "DoD Polygraph Program," December 24, 1984

(q) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982

(r) DoD Directive 5210.55, "Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities," July 6, 1977

(s) DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program (PRP)," May 25, 1993

(t) DoD Directive 5200.8, "Security of Military Installations and Resources," April 25,1991

(u) DoD 1401.1-M, "Personnel Policy Manual for Nonappropriated Fund Instrumentalities," January 1981, authorized by DoD Instruction 1401.1, November 15, 1985

(v) DoD 5030.49-R, "Customs Inspection," May 1977, authorized by DoD Directive 5030.49, January 6, 1984

(w) DoD Instruction 5210.25, "Assignment of American National Red Cross and United Service Organizations, Inc., Employees to Duty with the Military Services," May 12, 1983

(x) DoD Directive 5210.46, "DoD Building Security for the National Capital Region," January 28, 1982

(y) DoD Directive 5210.65, "Chemical Agent Security Program," October 15, 1986

(z) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978

(aa) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988

(bb) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982

(cc) 5 CFR, Part 732, "National Security Positions," January 1, 1995

(dd) Section 3571 of title 5, United States Code

(ee) Section 3 of Public Law 89-380, "Back Pay Act of 1966," March 30, 1966 (80 Stat. 94)

(ff) Executive Order 9835, "Prescribing Procedures for the Administration of an Employee Loyalty Program in the Executive Branch of the Government," issued 1947 (superseded by Executive Order 10450)

(gg) Public Law 83-703, "Atomic Energy Actof 1954," as amended, August 30, 1954

(hh) DoD Directive 5105.42, "Defense Investigative Service," June 14, 1985

(ii) Defense Investigative Service 20-1-M, "Manual for Personnel Security Investigations," January 1993

(jj) Memorandum of Understanding between the Director, White House Military Office and the Special Assistant to the Secretary and Deputy Secretary of Defense, "White House Clearances," July 30, 1980

(kk) USSAN Instruction 1-69, April 21, 1982 (Enclosure 2 to DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982

(ll) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1982

(mm) DoD Directive 5100.3, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands," November 1, 1988

(nn) Public Law 96-456, "Classified Information Procedures Act," October 15, 1980 (94 Stat. 2025)

(oo) DoD Directive 5142.1, "Assistant Secretary of Defense (Legislative Affairs)," July 2, 1982

(pp) Section 7532 of title 5, United States Code

(qq) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 4, 1989

(rr) National Security Directive 63, "Single Scope Background Investigations," October 21, 1991

DL1. DEFINITIONS

DL1.1.1. Access. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified informaiton by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

DL1.1.2. Adverse Action. A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

DL1.1.3. Background Investigation (BI). A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph AP1.1.1.3., Appendix 1, this Regulation, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

DL1.1.4. Classified Informaiton. Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356 (reference (j)).

DL1.1.5. Defense Central Security Index (DCSI). An automated sub-system of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all DoD Components for military, civilian, and contractor personnel. The DCSI will serve as the central DoD repository of security related actions in order to assist DoD security officials in making sound clearance and access determinations. The DCSI shall also serve to provide accurate and reliable statistical data for senior DoD officials, Congressional committees, the General Accounting Office and other authorized Federal requesters.

DL1.1.6. DoD Component. Includes the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, The DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

DL1.1.7. Entrance National Agency Check (ENTNAC). A personnel security

investigation scoped and conducted in the same manner as a National Agency Check (NAC) except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

DL1.1.8. Head of DoD Component. The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of the Combatant Commands; and the Directors of Defense Agencies.

DL1.1.9. Immigrant Alien. Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

DL1.1.10. Interim Security Clearance. A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

DL1.1.11. Limited Access Authorization. Authorization for access to Confidential or Secret information granted to non-United States citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (paragraph AP1.1.1.3., Appendix 1).

DL1.1.12. Minor Derogatory Information. Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

DL1.1.13. National Agency Check (NAC). A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph AP1.1.1.1., Appendix 1, this Regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

DL1.1.14. National Agency Check Plus Written Inquiries (NACI). A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

DL1.1.15. DoD National Agency Check Plus Written Inquiries (DNACI). A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a NAC, credit bureau check, and written inquiries to current and former employers (see paragraph AP1.1.1.2., Appendix 1), covering a 5-year scope.

DL1.1.16. National Security. National security means the national defense and foreign relations of the United States.

DL1.1.17. Need-to-Know A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

DL1.1.18. Periodic Reinvestigation (PR). An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs C3.7. through C3.7.10. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent 5-year period.

DL1.1.19. Personnel Security Investigation (PSI). Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see paragraph C2.4.3.) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

DL1.1.20. Scope The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

DL1.1.21. Security Clearance. A determination that a person is eligible under the

standards of this Regulation for access to classified information.

DL1.1.22. Senior Officer of the Intelligence Community (SOIC). The DoD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; Assistant Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

DL1.1.23. Sensitive Position. Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive as described in paragraph C3.1.1.

DL1.1.24. Significant Derogatory Information. Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

DL1.1.25. Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need-to-know.

DL1.1.26. Special Background Investigation (SBI). A personnel security investigation consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph AP1.1.1.4., Appendix 1, this Regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

DL1.1.27. Special Investigative Inquiry (SII). A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provision of this Regulation.

DL1.1.28. Service. Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DoD contractor or as a consultant involving access under the DoD Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

DL1.1.29. Unfavorable Administrative Action. Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this Regulation.

DL1.1.30. Unfavorable Personnel Security Determination. A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring a trustworthiness determination under this Regulation; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

DL1.1.31. United States Citizen. (Native Born) - A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or the Republic of Panama (former Panama Canal Zone) (if the father or mother (or both) was or is, a citizen of the United States).

C1. CHAPTER 1

DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM GENERAL PROVISIONS

C1.1. PURPOSE AND APPLICABILITY

C1.1. Purpose

C1.1.1. To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense, and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.

C1.1.2. This Regulation:

C1.1.2.1. Establishes DoD personnel security policies and procedures;

C1.1.2.2. Sets forth the standards, critera, and guidelines upon which personnel security determinations shall be based;

C1.1.2.3. Prescribes the kinds and scopes of personnel security investigations required;

C1.1.2.4. Details the evaluation and adverse action procedures by which personnel security determinations shall be made; and

C1.1.2.5. Assigns overall program management responsibilities.

C1.2. Applicability

C1.2.1. This Regulation implements the Department of Defense Personnel Security Program and takes precedence over all other departmental issuances affecting that program.

C1.2.2. All provisions of this Regulation apply to DoD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, contractor personnel and other personnel who are affiliated with the Department of Defense except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DoD 5220.22-R

(reference (b)) and in DoD Directive 5220.6 (reference (c)).

C1.2.3. The policies and procedures THAT govern the National Security Agency are prescribed by Public Laws 88-290 and 86-36, Executive Orders 10450 and 12333, DoD Directive 5210.45, Director of Central Intelligence Directive (DCID) 1/14 (references (e), (f), (g), (h), (i), and (l) respectively), and regulations of the National Security Agency.

C1.2.4. Under combat conditions or other military exigencies, an authority in paragraph AP6.1., Appendix 6, may waive such-provisions of this regulation as the circumstances warrant.

C2. CHAPTER 2

POLICIES

C2.1. STANDARDS FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES

C2.1.1. General. Only United States citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless an authority designated in Appendix 6 has determined that, based on all available information, there are compelling reasons in furtherance of the Department of Defense mission, including, special expertise, to assign an individual who is not a citizen to sensitive duties or grant a Limited Access Authorization to classified information. Non-U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by the Office of Personnel Management, pursuant to E.O. 11935 (reference (k)). Exceptions to these requirements shall be permitted only for compelling national security reasons.

C2.1.2. Clearance and Sensitive Position Standard. The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

C2.1.3. Military Service Standard. The personnel security standard that must be applied in determining whether a person is suitable under national security criteria for appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

C2.2. CRITERIA FOR APPLICATION OF SECURITY STANDARDS

C2.2.1. Criteria for Application of Security Standards. The ultimate decision in applying either of the security standards set forth in paragraph C2.1.2. and C2.1.3., above, must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance under the security standard shall include, but not be limited to the following:

C2.2.1.1. Commission of any act of sabotage, espionage, treason, terrorism,

anarchy, sedition, or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

C2.2.1.2. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar 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 to alter the form of Government of the United States by unconstitutional means.

C2.2.1.3. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

C2.2.1.4. 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 (hereafter 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.

C2.2.1.5. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by Statute, Executive Order or Regulation.

C2.2.1.6. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serve or which could be expected to serve the interests of another government in reference to the interests of the United States.

C2.2.1.7. Disregard of public law, Statutes, Executive Orders or Regulations including violation of security regulations or practices.

C2.2.1.8. Criminal or dishonest conduct.

C2.2.1.9. Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.

C2.2.1.10. Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.

C2.2.1.11. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be:

C2.2.1.11.1. The presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States; or

C2.2.1.11.2. Any other circumstances that could cause the applicant to be vulnerable.

C2.2.1.12. Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

C2.2.1.13. Habitual or episodic use of intoxicants to excess.

C2.2.1.14. Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

C2.2.1.15. Any knowing and willful falsification, cover up, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal Agency.

C2.2.1.16. Failing or refusing to answer or-to-authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment.

C2.2.1.17. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.

C2.3. TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS

C2.3.1. General. The types of personnel security investigations authorized below vary in scope of investigative effort required to meet the purpose of the particular investigation. No other types are authorized. The scope of a PSI may be neither raised nor lowered without the approval of the Deputy Under Secretary of Defense for Policy.

C2.3.2. National Agency Check (NAC) Essentially, a NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making a personnel security determination. An ENTNAC is a NAC (scope as outlined in paragraph AP1.1.1., Appendix 1) conducted on inductees and first-term enlistees, but lacking a technical fingerprint search. A NAC is also an integral part of each BI, SBI, and Periodic Reinvestigation (PR). Chapter 3 prescribes when a NAC is required.

C2.3.3. National Agency Check plus Written Inquiries. The Office of Personnel Management (OPM) conducts a NAC plus Written Inquiries (NACIs) on civilian employees for all Departments and Agencies of the Federal Government, pursuant to E.O. 10450 (reference (g)). NACIs are considered to meet the investigative requirements of this Regulation for a nonsensitive or noncritical sensitive position and/or up to a SECRET clearance and, in addition to the NAC, include coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last 5 years.

C2.3.4. DoD National Agency Check (DNCI) Plus Written Inquiries. DIS will conduct a DNACI, consisting of the scope contained in paragraph AP1.1.1.1.2., Appendix 1, for DoD military and contractor personnel for access to SECRET information. Chapter 3 prescribes when a DNACI is required.

C2.3.5. Background Investigation (BI). The BI is the principal type of investigation conducted when an individual requires TOP SECRET clearance or is to be assigned to a critical sensitive position. The BI normally covers a 5-year period and consists of a subject interview, NAC, LACs, credit checks, developed character references (3), employment records checks, employment references (3), and select scoping as required to resolve unfavorable or questionable information. (See paragraph AP1.1.1.1.3., Appendix 1). Chapter 3 prescribes when a BI is required.

C2.3.6. Special Background Investigation (SBI)

C2.3.6.1. An SBI is essentially a BI providing additional coverage both in

period of time as well as sources of information, scoped in accordance with the provisions of DCID 1/14 (reference (l)) but without the personal interview. While the kind of coverage provided for by the SBI determines eligibility for access to SCI, the Department of Defense has adopted this coverage for certain other Special Access programs. Chapter 3 prescribes when an SBI is required.

C2.3.6.2. The OPM, FBI, Central Intelligence Agency (CIA), Secret Service, and the Department of State conduct specially scoped BIs under the provisions of DCID 1/14. Any investigation conducted by one of the above-cited Agencies under DCID 1/14 standards is considered to meet the SBI investigative requirements of this Regulation.

C2.3.6.3. The detailed scope of an SBI is set forth in paragraph AP1.1.1.1.4., Appendix 1.

C2.3.7. Special Investigative Inquiry (SII)

C2.3.7.1. A Special Investigative Inquiry is a personnel security investigation conducted to prove or disprove allegations relating to the criteria outlined in paragraph C2.2.1. of this Regulation, except current criminal activities (see paragraph C2.4.3.4.), that have arisen concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a trustworthiness determination.

C2.3.7.2. Special Investigative Inquiries are scoped as necessary to address the specific matters requiring resolution in the case concerned and generally consist of record checks and/or interviews with potentially knowledgeable persons. An SII may include an interview with the subject of the investigation when necessary to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information.

C2.3.7.3. In those cases when there is a disagreement between Defense Investigative Service (DIS) and the requester as to the appropriate scope of the investigation, the matter may be referred to the Deputy Under Secretary of Defense for Policy for resolution.

C2.3.8. Periodic Reinvestigation (PR). As referred to in paragraph C3.7.1. and other national directives, certain categories of duties, clearance, and access require the conduct of a PR every five years according to the scope outlined in paragraph AP1.1.1.1.5., Appendix 1. The PR scope applies to military, civilian, contractor, and foreign national personnel.

C2.3.9. Personal Interview. Investigative experience over the years has demonstrated that, given normal circumstances, the subject of a personnel security investigation is the best source of accurate and relevant information concerning the matters under consideration. Further, restrictions imposed by the Privacy Act of 1974 (reference (m)) dictate that Federal investigative agencies collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. Accordingly, personal interviews are an integral part of the DoD personnel security program and shall be conducted in accordance with the requirements set forth in the following paragraphs of this section.

C2.3.9.1. BI/PR. A personal interview shall be conducted by a trained DIS agent as part of each BI and PR.

C2.3.9.2. Resolving Adverse Information. A personal interview of the subject shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations), when necessary, as part of each Special Investigative Inquiry, as well as during the course of initial or expanded investigations, to resolve or clarify any information which may impugn the subject's moral character, threaten the subject's future federal employment, raise the question of subject's security clearability, or be otherwise stigmatizing.

C2.3.9.3. Hostage Situation. A personal interview shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations) in those instances in which an individual has immediate family members or other persons bound by ties of affection or obligation who reside in a nation whose interests are inimical to the interests of the United States. (See paragraph C2.4.4.)

C2.3.9.4. Applicants/Potential Nominees for DoD Military or Civilian Positions Requiring Access to SCI or Other Positions Requiring SBI. A personal interview of the individual concerned shall be conducted, to the extent feasible, as part of the selection process for applicants/potential nominees for positions requiring access to SCI or completion of an SBI. The interview shall be conducted by a designee of the Component to which the applicant or potential nominee is assigned. Clerical personnel are not authorized to conduct these interviews. Such interviews shall be conducted utilizing-resources in the order of priority indicated below:

C2.3.9.4.1. Existing personnel security screening systems (e.g., Air Force

Assessment Screening Program, Naval Security Group Personnel Security Interview Program, U.S. Army Personnel Security Screening Program); or

C2.3.9.4.2. Commander of the nominating organization or such official as he or she has designated in writing (e.g., Deputy Commander, Executive Officer, Security Officer, Security Manager, S-2, Counterintelligence Specialist, Personnel Security Specialist, or Personnel Officer); or

C2.3.9.4.3. Agents of investigative agencies in direct support of the DoD Component concerned.

C2.3.9.5. Administrative Procedures

C2.3.9.5.1. The personal interview required by paragraph C2.3.9.4., above, shall be conducted in accordance with Appendix 6.

C2.3.9.5.2. For those investigations requested subsequent to the personal interview requirements of paragraph C2.3.9.4., above, the following procedures apply:

C2.3.9.5.2.1. The DD Form 1879 (Request for Personnel Security Investigation) shall be annotated under Item 20 (Remarks) with the statement, "Personal Interview Conducted by (cite the duty assignment of the designated official (e.g., Commander, Security Officer, Personnel Security Specialist, etc.))" in all cases in which an SBI is subsequently requested.

C2.3.9.5.2.2. Unfavorable information developed through the personal interview required by paragraph C2.3.9.4., above, will be detailed in a written report attached to the DD Form 1879 to include full identification of the interviewer. Failure to provide such information may result in conduct of an incomplete investigation by DIS.

C2.3.9.5.2.3. Whenever it is determined that it is not feasible to conduct the personal interview required by paragraph C2.3.9.4., above, prior to requesting the SBI, the DD Form 1879 shall be annotated under Item 20 citing the reason for not conducting the interview.

C2.3.10. Expanded Investigation. If adverse or questionable information relevant to a security determination is developed during the conduct of a personnel security investigation, regardless of type, the investigation shall be expanded, consistent with the restrictions in paragraph C2.5.5., to the extent necessary to substantiate or disprove the adverse or questionable information.

C2.4. AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES

C2.4.1. Genera. The DIS provides a single centrally directed personnel security investigative service to conduct personnel security investigations within the 50 States, District of Columbia, and Commonwealth of Puerto Rico for DoD Components, except as provided for in DoD Directive 5100.23 (reference (n)). DIS will request the Military Departments or other appropriate Federal Agencies to accomplish DoD investigative requirements in other geographic areas beyond their jurisdiction. No other DoD Component shall conduct personnel security investigations unless specifically authorized by the Deputy Assistant Secretary of Defense (Intelligence and Security). In certain instances provided for below, the DIS shall refer an investigation to other investigative agencies.

C2.4.2. Subversive Affiliations

C2.4.2.1. General. In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:

C2.4.2.1.1. Overthrowing the Government of the United States or the government of a State;

C2.4.2.1.2. Substantially impairing for the purpose of influencing U.S. Government policies or decisions:

C2.4.2.1.2.1. The functions of the Government of the United States, or

C2.4.2.1.2.2. The functions of the government of a State;

C2.4.2.1.2.3. Depriving persons of their civil rights under the Constitution or laws of the United States.

C2.4.2.2. Military Department/FBI Jurisdiction. Allegations of activities covered by criteria C2.2.1.1. through C2.2.1.6. of paragraph C2.2.1. of this Regulation are in the exclusive investigative domain of either the counterintelligence agencies of the Military Departments or the FBI, depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI (reference (o)). Whenever

allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a personnel security investigation conducted by DIS, they shall be referred immediately to either the FBI or to a Military Department counterintelligence agency as appropriate.

C2.4.2.3. DIS Jurisdiction. Allegations of activities limited to those set forth in criterion C2.2.1.7. through C2.2.1.17. of paragraph C2.2.1. of this Regulation shall be investigated by DIS.

C2.4.3. Suitability Information

C2.4.3.1. General. Most derogatory information developed through personnel security investigations of DoD military or civilian personnel is so-called suitability information, that is, information pertaining to activities or situations covered by criteria C2.2.1.7. through C2.2.1.17. of paragraph C2.2.1. of this Regulation. Almost all unfavorable personnel security determinations made by DoD authorities are based on derogatory suitability information, although such information is often used as a basis for unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice or removal from Federal employment under OPM regulations.

C2.4.3.2. Pre-Clearance Investigation. Derogatory suitability information, except that covered in C2.4.3.4., below, developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel security clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to criteria C2.2.1.7. through C2.2.1.17. of paragraph C2.2.1.

C2.4.3.3. Postjudicative Investigation. Derogatory suitability allegations, except those covered by C2.4.3.4., below, arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified information, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a Special Investigative Inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior shall also be referred to DIS for investigation. In such cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when paragraph C3.7.2. applies. Post adjudication investigation of allegations of a suitability nature required to support other types of unfavorable personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable Component administrative regulations. These latter categories of allegations

lie outside the DoD personnel security program and are not a proper investigative function for departmental counterintelligence organizations, Component personnel security authorities, or DIS.

C2.4.3.4. Allegations of Criminal Activity. Allegations of possible criminal conduct arising during a personnel security investigation shall be referred to the appropriate Department of Defense criminal investigative agency, Military Department or civilian jurisdiction unless the limitations in paragraph C2.4.3.4.1. through C2.4.3.4.3., below, apply. Where the allegation concerns a potential violation of the Uniform Code of Military Justice, Military Department investigative agencies have primary investigative jurisdiction. The following limitations apply to referrals to all law enforcement agencies, both military and civilian.

C2.4.3.4.1. Allegations shall not be referred or reported to law enforcement agencies where agreements with the agency or in cases where there is no agreement, past experience indicates that the jurisdiction does not have a substantial interest in prosecution of the offense or in receiving reports of the offense either due to the type or offense involved or the circumstances under which it occurred.

C2.4.3.4.2. Allegations about private consensual sexual acts with adults shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. That limitation does not apply to allegations that an individual attempted, solicited, or committed a criminal offense in the following circumstances:

C2.4.3.4.2.1. By using force, coercion, or intimidation.

C2.4.3.4.2.2. With a person under 17 years of age.

C2.4.3.4.2.3. Openly in public view.

C2.4.3.4.2.4. For compensation or with an offer of compensation to another individual.

C2.4.3.4.2.5. While on active duty in, or on duty in a Reserve component of, the Armed Forces of the United States, and

C2.4.3.4.2.5.1. Aboard a military vessel or aircraft; or

C2.4.3.4.2.5.2. With a subordinate in circumstances that violate customary military superior-subordinate relationships.

Exceptions to that limitation will be made only with the specific written authorization of the General Counsel of the Department of Defense, or his or her designee.

C2.4.3.4.3. Information about an individual's sexual orientation or statements by an individual that he or she is a homosexual or bisexual, or words to that effect, shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. If investigative reports containing such information are referred to law enforcement agencies or Military Departments for other reasons, information subject to the limitations in this paragraph will be removed.

C2.4.4. Hostage Situations

C2.4.4.1. General. A hostage situation exists when a member of subjects immediate family or such other person to whom the individual is bound by obligation or affection resides in a country whose interests are inimical to the interests of the United States. The rationale underlying this category of investigation is based on the possibility that an individual in such a situation might be coerced, influenced, or pressured to act contrary to the interests of national security.

C2.4.4.2. DIS Jurisdiction. In the absence of evidence of any coercion, influence or pressure, hostage investigations are exclusively a personnel security matter, rather than counterintelligence, and all such investigations shall be conducted by DIS.

C2.4.4.3. Military Department and/or FBI Jurisdiction. Should indications be developed that hostile intelligence is taking any action specifically directed against the individual concerned, or should there exist any other evidence that the individual is actually being coerced, influenced, or pressured by an element inimical to the interests of national security, then the case becomes a counter intelligence matter (outside of investigative jurisdiction of DIS) to be referred to the appropriate Military Department

or the FBI for investigation.

C2.4.5. Overseas Personnel Security Investigations. Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate Military Department investigative organization. Only post adjudication investigations involving an overseas subject may be referred by the requester directly to the Military Department investigative organization having investigative responsibility in the overseas area concerned (see Appendix 9) with a copy of the investigative request sent to DIS. In such cases, the Military Department investigative agency will complete the investigation, forward the completed report of investigation directly to DIS, with a copy to the requester.

C2.5. LIMITATIONS AND RESTRICTIONS

C2.5.1. Authorized Requesters and Personnel Security Determination Authorities. Personnel security investigations may be requested and personnel security clearances (including Special Access authorizations as indicated) granted only by those authorities designated in paragraph C5.1.2. and Appendix 5.

C2.5.2. Limit Investigations and Access. The number of persons cleared for access to classified information shall be kept to a minimum, consistent with the requirements of operations. Special attention shall be given to eliminating unnecessary clearances and requests for personnel security investigations.

C2.5.3. Collection of Investigative Data. To the greatest extent practicable, personal information relevant to personnel security determinations shall be obtained directly from the subject of a personnel security investigation. Such additional information required to make the necessary personnel security determination shall be obtained as appropriate from knowledgeable personal sources, particularly subjects peers, and through checks of relevant records including school, employment, credit, medical, and law enforcement records.

C2.5.4. Privacy Act Notification. Whenever personal information is solicited from an individual preparatory to the initiation of a personnel security investigation, the individual must be informed of:

C2.5.4.1. The authority (statute or Executive Order that authorized solicitation);

C2.5.4.2. The principal purpose or purposes for which the information is to be used;

C2.5.4.3. The routine uses to be made of the information;

C2.5.4.4. Whether furnishing such information is mandatory or voluntary;

C2.5.4.5. The effect on the individual, if any, of not providing the information; and

C2.5.4.6. That subsequent use of the data may be employed as part of an a periodic, random process to screen and evaluate continued eligibility for access to classified information.

C2.5.5. Restrictions on Investigators. Investigations shall be carried out insofar as possible to collect only as much information as is relevant and necessary for a proper personnel security determination. Questions concerning personal and domestic affairs, national origin, financial matters, and the status of physical health should be avoided unless the question is relevant to the criteria of paragraph C2.2.1. of this Regulation. Similarly, the probing of a person's thoughts or beliefs and questions about conduct that have no personnel security implications are unwarranted. When conducting investigations under the provisions of this Regulation, investigators shall:

C2.5.5.1. Investigate only cases or persons assigned within their official duties.

C2.5.5.2. Interview sources only where the interview can take place in reasonably private surroundings.

C2.5.5.3. Always present credentials and inform sources of the reasons for the investigation.. Inform sources of the subjects accessibility to the information to be provided and to the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisements to subjects of personnel security investigations are outlined in paragraph C2.5.4., above.

C2.5.5.4. Furnish only necessary identity data to a source, and refrain from asking questions in such a manner as to indicate that the investigator is in possession of derogatory information concerning the subject of the investigation.

C2.5.5.5. Refrain from using, under any circumstances, covert or surreptitious investigative methods, devices, or techniques including mail covers, physical or photographic surveillance, voice analyzers, inspection of trash, paid informants, wiretap, or eavesdropping devices.

C2.5.5.6. Refrain from accepting any case in which the investigator knows of circumstances that might adversely affect his fairness, impartiality, or objectivity.

C2.5.5.7. Refrain, under any circumstances, from conducting physical searches of subject or his property.

C2.5.5.8. Refrain from attempting to evaluate material contained in medical files. Medical files shall be evaluated for personnel security program purposes only by such personnel as are designated by DoD medical authorities. However, review and collection of medical record information may be accomplished by authorized investigative personnel.

C2.5.6. Polygraph Restrictions. The polygraph may be used as a personnel security screening measure only in those limited instances authorized by the Secretary of Defense in DoD Directive 5210.48, (reference (p)).

C3. CHAPTER 3

PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

C3.1. SENSITIVE POSITIONS

C3.1.1. Designation of Sensitive Positions. Certain civilian positions within the Department of Defense entail duties of such a sensitive nature including access to classified information, that the misconduct, malfeasance, or nonfeasance of an incumbent in any such position could result in an unacceptably adverse impact upon the national security. These positions are referred to in this Regulation as sensitive positions. It is vital to the national security that great care be exercised in the selection of individuals to fill such positions. Similarly, it is important that only positions which truly meet one or more of the criteria set forth in paragraph C3.1.2., below, be designated as sensitive.

C3.1.2. Criteria for Security Designation of Positions. Each civilian position within the Department of Defense shall be categorized, with respect to security sensitivity, as either nonsensitive, noncritical-sensitive, or critical-sensitive.

C3.1.2.1. The criteria to be applied in designating a position as sensitive are:

C3.1.2.1.1. Critical-sensitive

C3.1.2.1.1.1. Access to Top Secret information.

C3.1.2.1.1.2. Development or approval of plans, policies, or programs that affect the overall operations of the Department of Defense or of a DoD Component.

C3.1.2.1.1.3. Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

C3.1.2.1.1.4. Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.

C3.1.2.1.1.5. Fiduciary, public contact, or other duties demanding the highest degree of public trust.

C3.1.2.1.1.6. Duties falling under Special Access programs.

C3.1.2.1.1.7. Category I automated data processing (ADP) positions.

C3.1.2.1.1.8. Any other position so designated by the Head of the DoD Component or designee.

C3.1.2.1.2. Noncritical-sensitive

C3.1.2.1.2.1. Access to Secret or Confidential information.

C3.1.2.1.2.2. Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DoD personnel and property.

C3.1.2.1.2.3. Category II automated data processing positions.

C3.1.2.1.2.4. Duties involving education and orientation of DoD personnel.

C3.1.2.1.2.5. Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DoD personnel and property.

C3.1.2.1.2.6. Any other position so designated by the Head of the DoD Component or designee.

C3.1.2.2. All other positions shall be designated as nonsensitive.

C3.1.3. Authority to Designate Sensitive Positions. The authority to designate sensitive positions is limited to those authorities designated in paragraph AP5.7., Appendix 5. These authorities shall designate each position within their jurisdiction as to its security sensitivity and maintain these designations current vis-a-vis the specific duties of each position.

C3.1.4. Limitation of Sensitive Positions. It is the responsibility of those authorities authorized to designate sensitive positions to insure that (1) only those positions are designated as sensitive that meet the criteria of paragraph C3.1.2. above and (2) that the designation of sensitive positions is held to a minimum consistent with

mission requirements. Designating authorities shall maintain an accounting of the number of sensitive positions by category, i.e., critical or non-critical sensitive. Such information will be included in annual report required in Chapter 9.

C3.1.5. Billet Control System For Top Secret

C3.1.5.1. To standardize and control the issuance of Top Secret clearances within the Department of Defense, a specific designated billet must be established and maintained for all DoD military and civilian positions requiring access to Top Secret information. Only persons occupying these billet positions will be authorized a Top Secret clearance. If an individual departs from a Top Secret billet to a billet/position involving a lower level clearance, the Top Secret clearance will be administratively rescinded. This Top Secret billet requirement is in addition to the existing billet structure maintained for SCI access.

C3.1.5.2. Each request to DIS for a BI or SBI that involves access to Top Secret or SCI information will require inclusion of the appropriate billet reference, on the request for investigation. Each Component head should incorporate, to the extent feasible, the Top Secret billet structure into the component Manpower Unit Manning Document. Such a procedure should minimize the time and effort required to maintain such a billet structure.

C3.1.5.3. A report on the number of established Top Secret billets will be submitted each year to the DUSD(P) as part of the annual clearance report referred to in Chapter 11.

C3.2. CIVILIAN EMPLOYMENT

C3.2.1. General. The appointment of each civilian employee in any DoD Component is subject to investigation, except for reappointment when the break in employment is less than 12 months. The type of investigation required is set forth in this section according to position sensitivity.

C3.2.2. Nonsensitive Positions. In accordance with the OPM Federal Personnel Manual, (reference (cc)) a NACI shall be requested not later than 3 working days after a person is appointed to a nonsensitive position. Although there is normally no investigation requirement for per diem, intermittent, temporary or seasonal employees in nonsensitive positions provided such employment does not exceed an aggregate of 120 days in either a single continuous or series of appointments, a NAC may be requested of DIS where deemed appropriate by the employing activity.

C3.2.3. Noncritical-Sensitive Positions

C3.2.3.1. An NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical-sensitive position (for exceptions see paragraph C3.2.5.). An ENTNAC, NAC or DNACI conducted during military or contractor employment may also be used for appointment provided a NACI has been requested from OPM and there is no more than 12 months break in service since completion of the investigation.

C3.2.3.2. Seasonal employees (including summer hires) normally do not require access to classified information. For those requiring access to classified information the appropriate investigation is required. The request for the NAC (or NACI) should be submitted to DIS by entering "SH"(summer hire) in red letters approximately one inch high on the DD Form 398-2, "Personnel Security Questionnaire (National Agency Checklist)." Additionally, to ensure expedited processing by DIS, summer hire requests should be assembled and forwarded to DIS in bundles, when appropriate.

C3.2.4. Critical-Sensitive Positions. A BI shall be favorably completed prior to appointment to critical-sensitive positions (for exceptions see paragraph C3.2.5.). Certain critical-sensitive positions require a preappointment SBI in accordance with section C3.5. of this chapter. Preappointment BIs and SBIs will be conducted by DIS.

C3.2.5. Exceptions

C3.2.5.1. Noncritical-sensitive. In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made part of the record. In such instances, the position may be filled only after the NACI has been requested.

C3.2.5.2. Critical-sensitive. In an emergency, a critical-sensitive position may be occupied pending completion of the BI (or SBI, as appropriate) if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record. In such instances, the position may be filled only when the NAC portion of the BI (or SBI) or a previous valid NACI, NAC or ENTNAC has been completed and favorably adjudicated.

C3.2.6. Mobilization of DoD Civilian Retirees. The requirements contained in paragraph C3.2.1. of this section, regarding the type of investigation required by position sensitivity for DoD civilian retirees temporary appointment when the break in employment is greater than 12 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of Title 5, United States Code, depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to newly assigned personnel assigned to the defense intelligence and security agencies with respect to granting security clearances in an expeditious manner under paragraph C3.2.1. of this section.

C3.3. MILITARY APPOINTMENT, ENLISTMENT, AND INDUCTION

C3.3.1. General. The appointment, enlistment, and induction of each member of the Armed Forces or their Reserve components shall be subject to the favorable completion of a personnel security investigation. The types of investigation required are set forth in this section.

C3.3.2. Entrance Investigation

C3.3.2.1. An ENTNAC shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. A DNACI shall be conducted on each commissioned officer, except as permitted by paragraph C3.3.4. of this section, warrant officer, cadet, midshipman, and Reserve Officers Training Candidate, at the time of appointment. A full NAC shall be conducted upon reentry of any of the above when there has been a break in service greater than 12 months.

C3.3.2.2. If an officer or warrant officer candidate has been the subject of a favorable NAC or ENTNAC and there has not been a break in service of more than 12 months, a new NAC is not authorized. This includes ROTC graduates who delay entry onto active duty pending completion of their studies.

C3.3.2.3. All derogatory information revealed during the enlistment or apppointment process that results in a moral waiver will be fully explained on a written summary attached to the DD Form 398-2.

C3.3.3. Reserve Components and National Guard. Reserve component and National Guard personnel not on active duty are subject to the investigative requirements of this chapter.

C3.3.4. Exceptions for Certain Commissioned Officers of Reserve Components.

The requirements for entrance investigation shall be rigidly adhered to except as follows. Healthcare professionals, chaplains, and attorneys may be commissioned in the Reserve components prior to completion of a DNACI provided that:

C3.3.4.1. A DNACI is initiated at the time an application for a commission is received; and

C3.3.4.2. The applying health professional, chaplain, or attorney agrees in writing that, if the results of the investigation are unfavorable, he or she will be subject to discharge if found to be ineligible to hold a commission. Under this exception, commissions in Reserve Components other than the National Guard may be tendered to immigrant alien health professionals, chaplains, and attorneys.

C3.3.5. Mobilization of Military Retirees. The requirements contained in paragraph C3.3.2. of this section, regarding a full NAC upon reentry to active duty of any officer or enlisted regular/reserve military retiree or Individual Ready Reserve who has been separated from service for a period of greater than 12 months, should be waived for the purposes of partial or full mobilization under provisions of Title 10, (Title 14, pertaining to the U.S. Coast Guard as an element of the Navy) United States Code, to include the period of prescribed service refresher training. Particular priority should be afforded to military retirees mobilized and assigned to the defense intelligence and security agencies communities.

C3.4. SECURITY CLEARANCE

C3.4.1. General

C3.4.1.1. The authorities designated in paragraph AP5.1., Appendix 5 are the only authorities authorized to grant, deny or revoke DoD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.

C3.4.1.2. Military, DoD civilian, and contractor personnel who are employed by or serving in a consultant capacity to the Department of Defense, may be considered for access to classified information only when such access is required in connection with official duties. Such individuals may be granted either a final or interim personnel security clearance provided the investigative requirements set forth below are complied with, and provided further that all available information has been adjudicated and a finding made that such clearance would be clearly consistent with the interests of national security.

C3.4.2. Investigative Requirements for Clearance

C3.4.2.1. Top Secret

C3.4.2.1.1. Final Clearance:

C3.4.2.1.1.1. BI.

C3.4.2.1.1.2. Established billet per paragraph C3.1.5. (except contractors).

C3.4.2.1.2. Interim Clearance:

C3.4.2.1.2.1. Favorable NAC, ENTNAC, DNACI, or NACI completed.

C3.4.2.1.2.2. Favorable review of DD Form 398/SF-86/SF-171/DD Form 49.

C3.4.2.1.2.3. BI or SBI has been initiated.

C3.4.2.1.2.4. Favorable review of local personnel, base/military police, medical, and other security records as appropriate.

C3.4.2.1.2.5. Established billet per paragraph C3.1.5. (except contractors).

C3.4.2.1.2.6. Provisions of paragraph C3.2.5. have been met regarding civilian personnel.

C3.4.2.2. Secret

C3.4.2.2.1. Final Clearance:

C3.4.2.2.1.1. DNACI: Military (except first-term enlistees) and contractor employees.

C3.4.2.2.1.2. NACI: Civilian employees.

C3.4.2.2.1.3. ENTNAC: First-term enlistees.

C3.4.2.2.2. Interim Clearance:

C3.4.2.2.2.1. When a valid need to access Secret information is established, an interim Secret clearance may be issued in every case, provided that the steps outlined in subparagraphs C3.4.2.2.2.2. through C3.4.2.2.2.5., below, have been complied with.

C3.4.2.2.2.2. Favorable review of DD Form 398-2/SF-85/SF-171/DD Form 48.

C3.4.2.2.2.3. NACI, DNACI, or ENTNAC initiated.

C3.4.2.2.2.4. Favorable review of local personnel, base military police, medical, and security records as appropriate.

C3.4.2.2.2.5. Provisions of paragraph C3.2.5. have been complied with regarding civilian personnel.

C3.4.2.2.3. Confidential

C3.4.2.2.3.1. Final Clearance:

C3.4.2.2.3.1.1. NAC or ENTNAC: Military and contractor employees (except for Philippine national members of the United States Navy on whom a BI shall be favorably completed).

C3.4.2.2.3.1.2. NACI: Civilian employees (except for summer hires who may be granted a final clearance on the basis of a NAC).

C3.4.2.2.3.2. Interim Clearance

C3.4.2.2.3.2.1. Favorable review of DD Form 398-2/SF 85/SF 17 1/DD Form 48.

C3.4.2.2.3.2.2. NAC, ENTNAC or NACI initiated.

C3.4.2.2.3.2.3. Favorable review of local personnel, base military police, medical, and security records as appropriate.

C3.4.2.2.3.2.4. Provisions of paragraph C3.2.5. have been complied with regarding civilian personnel.

C3.4.2.2.4. Validity of Previously Granted Clearances: Clearances granted under less stringent investigative requirements retain their validity; however, if a

higher degree of clearance is required, investigative requirements of this Regulation will be followed.

C3.4.3. Access to Classified Information by Non-U.S. Citizens

C3.4.3.1. Only U.S. citizens are eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national. Such individuals may be granted a "Limited Access Authorization" (LAA) in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed in pursuit of a specific DoD requirement involving access to specified classified information for which a cleared or clearable U.S. citizen is not available.

C3.4.3.2. Limitations

C3.4.3.2.1. LAAs shall be limited only to individuals who have a special skill or technical expertise essential to the fulfillment of a DoD requirement that cannot reasonably be filled by a U.S. citizen.

C3.4.3.2.2. LAAs shall not be granted to personnel who perform routine administrative or other support duties, such as secretaries, clerks, drivers, or mechanics, unless it has been clearly established that those duties cannot be performed by a U.S. citizen.

C3.4.3.2.3. Personnel granted LAAs shall not be permitted uncontrolled access to areas where classified information is stored or discussed. Classified information shall be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

C3.4.3.2.4. LAA personnel shall not be designated as a courier or escort for classified material outside the location in which access is permitted unless they are accompanied by an appropriately cleared U.S. person.

C3.4.3.3. Authorized Access Levels

C3.4.3.3.1. LAAs may be granted only at the SECRET and CONFIDENTIAL level. LAAs for TOP SECRET are prohibited. Interim access is not authorized pending approval of a LAA.

C3.4.3.3.2. The information the non-U S. citizen may have access to must

be approved for release to the persons country or countries of citizenship, in accordance with DoD Directive 5230.11 (reference (ll)).

C3.4.3.3.3. Access to classified information shall be limited or related to a specific program or project; the LAA shall be canceled or rejustified as described herein upon completion of the program or project.

C3.4.3.3.4. Access to classified information outside the scope of the approved LAA shall be considered a compromise of classified information and shall be investigated, in accordance with DoD 5200.1-R (reference (q)).

C3.4.3.4. Requirements

C3.4.3.4.1. The LAA granting authority (Appendix 5) may consider issuing an LAA only after a written determination is made that access is essential for a critical mission and no U.S. citizen is available to perform the duties.

C3.4.3.4.2. When a non-U.S. citizen who is nominated for an LAA is a citizen of a country with which the United States has an agreement providing for security assurances based on that countries investigative requirements, which are commensurate with the standards provided herein, an LAA may be issued at the requisite level.

C3.4.3.4.3. In addition to the above, a favorably completed (within the last 5 years) and adjudicated SSBI is required prior to granting an LAA. If the SSBI cannot provide full investigative coverage, a polygraph examination (if there are no host country legal prohibitions) to resolve the remaining personnel security issues (see DoD Directive 5210.48 (reference (p))), must be favorably completed before granting access.

C3.4.3.4.4. If geographical, political or medical situations prevent the full completion of the SSBI or prevent the than full SSBI, a LAA may be granted only with approval of the ASD(C3I).

C3.4.3.4.5. If an LAA is withdrawn and the individual subsequently is considered for an LAA, the provisions of this paragraph shall apply concerning an SSBI and polygraph examination. The scope of the SSBI normally shall cover the period since the previous background investigation or 10 years, whichever is shorter.

C3.4.3.4.6. A PR shall be conducted on every individual with a LAA 5 years from the date of the last PR or SSBI, as appropriate.

C3.4.3.4.7. All requests for initial LAAs shall contain a detailed justification and plan describing the following:

C3.4.3.4.7.1. The location of the classified material (security containers) in relationship to the location of the foreign national.

C3.4.3.4.7.2. The compelling reason for not employing a cleared or clearable U.S. citizen.

C3.4.3.4.7.3. A synopsis of an annual continuing assessment program to evaluate the individuars continued trustworthiness and eligibility for access.

C3.4.3.4.7.4. A plan to control access to secure areas and to classified and controlled unclassified information.

C3.4.3.5. LAA Determination Authority

C3.4.3.5.1. LAA determinations may only be made by an official listed in paragraph AP5.2., Appendix 5. The designated single authorizing official for the Military Departments, the Combatant Commands, and the DIS precludes an LAA determination by any other official at the major command level, or equivalent.

C3.4.3.5.2. LAA determinations for employees of the Military Departments shall be the sole authority of the Secretary of the Military Department or a single designee such as the Service central adjudication facility. Field elements must submit their recommendations for access to the designated official for approval, along with affiliated information in support of the action.

C3.4.3.5.3. The Commander of a Combatant Command, or single designee (flag officer or civilian equivalent) responsible for implementation of the personnel security program, shall be authorized to issue, deny, or revoke an LAA. LAA determinations by the Combatant Commands shall be reported to the central adjudicative facility of the Military Department in accordance with the assigned responsibilities in DoD Directive 5100.3 (reference (mm)) for inclusion in the DCII.

C3.4.3.5.4. All LAA determinations, favorable and unfavorable, shall be entered into the DCII

C3.4.3.5.5. The administrative action procedures in Chapter 8 do not apply to LAA determinations.

C3.4.3.6. Record

C3.4.3.6.1. The LAA granting authority shall ensure that a record is

created on issuance and maintained for 5 years from the date the LAA ceases. The record shall include the following:

C3.4.3.6.1.1. The identity of the individual granted the LAA, to include the full name, date and place of birth, current citizenship(s), any SSN, and any national identifying number issued by the individual's country or countries of citizenship;

C3.4.3.6.1.2. The individual's status as an immigrant alien or foreign national; if an immigrant alien, the date and place such status was granted;

C3.4.3.6.1.3. The classification level of the LAA; i.e., SECRET or CONFIDENTIAL;

C3.4.3.6.1.4. Date and type of most recent background investigation or PR and the investigating Agency.

C3.4.3.6.1.5. Whether a polygraph examination was conducted; if so, the date and administering Agency for the most recent examination.

C3.4.3.6.1.6. The nature and identity of the classified program materials to which access is authorized and the precise duties performed.

C3.4.3.6.1.7. The compelling reasons for granting access to the information.

C3.4.3.6.2. All LAA SSBIs and PRs shall be conducted under the auspices of the DIS and shall comply with the requirements of Appendix 1. The DIS shall initiate leads to the respective Military Department investigative agencies overseas as well as the Department of State (DOS). The results of all investigations, to include those conducted by the DOS, shall be returned to the DIS for review and entry into the DCII and return to the designated granting official for adjudication. (To expedite matters, the investigation may be initiated locally provided the necessary paperwork has been submitted to the DIS for assignment of a case control number and initiation of such other checks as needed.)

C3.4.3.6.3. The Combatant Commands shall report LAAs they issue to the applicable DoD Component CAF for entry into the DCII. The Combatant Commands shall ensure that all investigative paperwork for the initiation of the SSBI or PR is submitted to the DIS through the designated single-approval authority responsible for adjudication and issuance of the LAA.

C3.4.3.6.4. All LAA nominees must agree to undergo a polygraph

examination at any time during the period the LAA is in effect, if there is no host-country legal prohibition.

C3.4.3.7. All LAAs shall be reviewed annually by the issuing component to determine if continued access is in compliance with DoD policy. A report on all LAAs in effect, including the data required in paragraph C3.4.3.6.1. shall be furnished to the DASD(I&S) within 60 days after the end of each fiscal year (see subsection C11.1.3., below).

C3.4.4. Access by Persons Outside the Executive Branch

C3.4.4.1. Access to classified information by persons outside the Executive Branch shall be accomplished in accordance with Chapter VII, DoD 5200.1-R (reference (q)). The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

C3.4.4.2. Members of the U.S. Senate and House of Representative do not require personnel security clearances. They may be granted access to DoD classified information that relates to matters under the jurisdiction of the respective Committees to which they are assigned and is needed to perform their duties in connection with such assignments.

C3.4.4.3. Congressional staff members requiring access to DoD classified information shall be processed for a security clearance in accordance with DoD Directive 5142.1 (reference (oo)) and the provisions of this Regulation. The Director, Washington Headquarters Services (WHS) will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and grant, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

C3.4.4.4. State governors do not require personnel security clearances. They may be granted access to specifically designated classified information, on a "need-to-know" basis, based upon affirmation by the Secretary of Defense or the Head of a DoD Component or single designee, that access, under the circumstances, serves the national interest. Staff personnel of a governor's office requiring access to classified information shall be investigated and cleared in accordance with the prescribed procedures of this Regulation when the Head of a DoD Component, or single designee, affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a "need-to-know" basis.

C3.4.4.5. Members of the U.S. Supreme Court, the Federal judiciary and the

Supreme Courts of the individual States do not require personnel security clearances. They may be granted access to DoD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

C3.4.4.6. Attorneys representing DoD military, civilian or contractor personnel requiring access to DoD classified information to properly represent their clients, shall normally be investigated by DIS and cleared in accordance with the prescribed procedures in paragraph C3.4.2. This shall be done upon certification of the General Counsel of the DoD Component involved in the litigation that access to specified classified information, on the part of the attorney concerned, is necessary to adequately represent his or her client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of paragraph C3.4.2., access may be granted with the written approval of an authority designated in Appendix 5 provided that as a minimum: (a) a favorable name check of the FBI and the DCII has been completed, and (b) a DoD Non-Disclosure Agreement has been executed. In post-indictment cases, after a judge has invoked the security procedures of the Classified Information Procedures Act (CIPA) (reference (m)), the Department of Justice may elect to conduct the necessary background investigation and issue the required security clearance, in coordination with the affected DoD Component.

C3.4.5. Restrictions on Issuance of Personnel Security Clearance. Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements.

Personnel security clearances shall normally not be issued:

C3.4.5.1. To persons in nonsensitive positions.

C3.4.5.2. To persons whose regular duties do not require authorized access to classified information.

C3.4.5.3. For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

C3.4.5.4. To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

C3.4.5.5. To persons working in shipyards whose duties do not require access to classified information.

C3.4.5.6. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

C3.4.5.7. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

C3.4.5.8. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

C3.4.5.9. To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

C3.4.5.10. To perimeter security personnel who have no access to classified information.

C3.4.5.11. To drivers, chauffeurs and food service personnel.

C3.4.6. Dual Citizenship. Persons claiming both United States and foreign

citizenship shall be processed: under paragraph C3.4.2., above, and adjudicated in accordance with the "Foreign Preference" standard in Appendix 8.

C3.4.7. One-Time Access. Circumstances may arise where an urgent operational or contractual exigency exists for cleared DoD personnel to have one-time or short duration access to classified information at a higher level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such situations, and only for compelling reasons in furtherance of the DoD mission, an authority referred to in subparagraph C3.4.7.1., below, may grant higher level access on a temporary basis subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level clearance. Procedures and conditions for effecting emergency one-time access to the next higher classification level are as follows:

C3.4.7.1. Authorization for such one-time access shall be granted by a flag or general officer, a general court martial convening authority or equivalent Senior Executive Service member, after coordination with appropriate security officials.

C3.4.7.2. The recipient of the one-time access authorization must be a U.S. citizen, possess a current DoD security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

C3.4.7.3. Such access, once granted, shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

C3.4.7.4. The employee to be afforded the higher level access shall have been continuously employed by a DoD Component or a cleared DoD contractor for the preceding 24-month period. Higher level access is not authorized for part-tune employees.

C3.4.7.5. Pertinent local records concerning the employee concerned shall be reviewed with favorable results.

C3.4.7.6. Whenever possible, access shall be confined to a single instance or at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of the granting authority is

required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be canceled at or before 90 days from original date of access.

C3.4.7.7. Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible for:

C3.4.7.7.1. Recording the higher-level information actually revealed,

C3.4.7.7.2. The date(s) such access is afforded, and

C3.4.7.7.3. The daily retrieval of the material accessed.

C3.4.7.8. Access at the next higher level shall not be authorized for COMSEC, SCI, NATO, or foreign government information.

C3.4.7.9. The exercise of this provision shall be used sparingly and repeat use within any 12 month period on behalf of the same individual is prohibited. The approving authority shall maintain a record containing the following data with respect to each such access approved:

C3.4.7.9.1. The name, and SSN of the employee afforded higher level access.

C3.4.7.9.2. The level of access authorized.

C3.4.7.9.3. Justification for the access, to include an explanation of the compelling reason to grant the higher level access and specifically how the DoD mission would be furthered.

C3.4.7.9.4. An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded.

C3.4.7.9.5. A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

C3.4.7.9.6. The approving authority's signature certifying C3.4.7.9.1. through C3.4.7.9.5., above.

C3.4.7.9.7. Copies of any pertinent briefings/debriefings administered to the employee.

C3.4.8. Access by Retired Flag and/or General Officers

C3.4.8.1. Upon determination by an active duty flag/general officer that there are compelling reasons, in furtherance of the Department of Defense mission, to grant a retired flag/general officer access to classified information in connection with a specific DoD program or mission, for a period not greater than 90 days, the investigative requirements of this Regulation may be waived. The access shall be limited to classified information at a level commensurate with the security clearance held at the time of retirement -- not including access to SCI.

C3.4.8.2. The flag/general officer approving issuance of the clearance shall, provide the appropriate DoD Component central clearance facility a written record to be incorporated into the DCII detailing:

C3.4.8.2.1. Full identifying data pertaining to the cleared subject;

C3.4.8.2.2. The classification of the information to which access was authorized.

C3.4.8.3. Such access may be granted only after the compelling reason and the specific aspect of the DoD mission which is served by granting such access has been detailed and under the condition that the classified materials involved are not removed from the confines of a Government installation or other area approved for storage of DoD classified information.

C3.5. SPECIAL ACCESS PROGRAMS

C3.5.1. General. It is the policy of the Department of Defense to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding established requirements are authorized only when mandated by statute, national regulations, or international agreement or Executive Order 12968 or its successor. In this connection, there are certain special access programs (SAPs) originating at the national or international level that require personnel security investigations and procedures of a special nature. Those programs and the special investigative requirements imposed by them are described in this section. A SAP is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to E. O. 12958

(reference (j)) and prior Executive Orders. DoD Directive O-5205.7 (reference (qq)) prescribes policy and procedures for establishment, administration and reporting of Departmental SAPs.

C3.5.2. Sensitive Compartmented Information (SCI)

C3.5.2.1. The investigative requirements for access to SCI is an SBI (see paragraph AP1.1.1.4., Appendix 1) including a NAC on the individual's spouse or cohabitant. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudication agency that the Personnel Security standards of DCID 1/14 (reference (l)) are met.

C3.5.2.2. A previous investigation conducted within the past five years which substantially meets the investigative requirements prescribed by this section may serve as a basis for granting access approval provided that there has been no break in the individuals Military Service, DoD civilian employment, or access to classified information under the Industrial Security Program greater than 24 months. The individual shall submit one copy of an updated PSQ covering the period since the completion of the last SBI and/or SSBI and certify any substantive changes that may have occurred.

C3.5.2.3. In accordance with DCID 1/14 (reference (l)), a TOP SECRET security clearance shall not be a prerequisite for access to SCI. Determination of eligibility for access to SCI under reference (l) shall include eligibility for access to TOP SECRET and below.

C3.5.3. Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI). The investigative requirement for access to SIOP-ESI is an SBI, including a NAC on the spouse and the individual's immediate family who are 18 years of age or over and who are United States citizens other than by birth or who are resident aliens.

C3.5.4. Presidential Support Activities

C3.5.4.1. DoD Directive 5210.55 (reference (r)) prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DoD military and civilian personnel and contractor employees assigned to or utilized in Presidential Support activities. The type of investigation of individuals assigned to Presidential Support activities varies according to whether the person investigated qualifies for Category One or Category Two as indicated below:

C3.5.4.1.1. Category One

C3.5.4.1.1.1. Personnel assigned on a permanent or full-time basis to duties in direct support of the President (including the office staff of the Director, White House Military Office, and all individuals under his control):

C3.5.4.1.1.1.1. Presidential air crew and associated maintenance and security personnel.

C3.5.4.1.1.1.2. Personnel assigned to the White House communications activities and the Presidential retreat.

C3.5.4.1.1.1.3. White House transportation personnel.

C3.5.4.1.1.1.4. Presidential mess attendants and medical personnel.

C3.5.4.1.1.1.5. Other individuals filling administrative positions at the White House.

C3.5.4.1.1.2. Personnel assigned on a temporary or part-time basis to duties supporting the President:

C3.5.4.1.1.2.1. Military Social Aides.

C3.5.4.1.1.2.2. Selected security, transportation, flight-line safety, and baggage personnel.

C3.5.4.1.1.2.3. Others with similar duties.

C3.5.4.1.1.3. Personnel assigned to the Office of the Military Aide to the Vice President.

C3.5.4.1.2. Category Two

C3.5.4.1.2.1. Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential functions and facilities.

C3.5.4.1.2.2. Employees of contractors who provide services or contractors employees who require unescorted access to Presidential Support areas, activities, or equipment-including maintenance of the Presidential retreat communications, and aircraft.

C3.5.4.1.2.3. Individuals in designated units requiring a lesser degree of access to the President or Presidential Support activities.

C3.5.4.2. Personnel nominated for Category One duties must have been the subject of an SBI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The SBI must have been completed within the 12 months preceding selection for Presidential Support duties. If such an individual marries subsequent to the completion of the SBI, the required spouse check shall be made at that time.

C3.5.4.3. Personnel nominated for Category Two duties must have been the subject of a BI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The BI must have been completed within the 12 months preceding selection for Presidential Support duties. It should be noted that duties (separate and distinct from their Presidential Support responsibilities) of some Category Two personnel may make it necessary for them to have special access clearances, which require an SBI.

C3.5.4.4. The U.S. citizenship of foreign-born immediate family members of all Presidential Support nominees must be verified by investigation.

C3.5.4.5. A limited number of Category One personnel having especially sensitive duties have been designated by the Director, White House Military Office as "Category A." These personnel shall be investigated under special scoping in accordance with the requirements of reference (ii).

C3.5.5. Nuclear Weapon Personnel Reliabilily Program (PRP)

C3.5.5.1. DoD Directive 5210.42 (reference (s)) sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and nuclear components. The investigative requirement for personnel performing such duties is:

C3.5.5.1.1. Critical Position: BI. In the event that it becomes necessary to consider an individual for a critical position and the required BI has not been completed, interim certification may be made under carefully controlled conditions as set forth below.

C3.5.5.1.1.1. The individual has had a favorable DNACI, NAC (or

ENTNAC) within the past 5 years without a break in service or employment in excess of 1 year.

C3.5.5.1.1.2. The BI has been requested.

C3.5.5.1.1.3. All other requirements of the PRP screening process have been fulfilled.

C3.5.5.1.1.4. The individual is identified to supervisory personnel as being certified on an interim basis.

C3.5.5.1.1.5. The individual is not used in a two-man team with another such individual.

C3.5.5..1.1.6. Justification of the need for interim certification is documented by the certifying official.

C3.5.5.1.1.7. Should the BI not be completed within 150 days from the date of the request, the certifying official shall query the Component clearance authority, who shall ascertain from DIS the status of the investigation. On the basis of such information, the certifying official shall determine whether to continue or to withdraw the interim certification.

C3.5.5.1.2. Controlled Position: DNACI/NACI

C3.5.5.1.2.1. An ENTNAC completed for the purpose of first term enlistment or induction into the Armed Forces does not satisfy this requirement.

C3.5.5.1.2.2. interim certification is authorized for an individual who has not had a DNACI/NACI completed within the past 5 years, subject to the following conditions:

C3.5.5.1.2.2.1. The individual has had a favorable ENTNAC/NAC, or higher investigation, that is more than 5 years old and has not had a break in service or employment in excess of 1 year.

C3.5.5.1.2.2.2. A DNACI/NACI has been requested at the time of interim certification.

C3.5.5.1.2.2.3. All other requirements of the PRP screening process have been fulfilled.

C3.5.5.1.2.2.4. Should the DNACI/NACI not be completed within 90 days from the date of the request, the procedures set forth in C3.5.5.1.1.7., above, for ascertaining the delay of the investigation in the case of a critical position shall apply.

C3.5.5.1.2.3. Additional requirements apply.

C3.5.5.1.2.3.1. The investigation upon which certification is based must have been completed within the last 5 years from the date of initial assignment to a PRP position and there must not have been a break in service or employment in excess of 1 year between completion of the investigation and initial assignment.

C3.5.5.1.2.3.2. In those cases in which the investigation was completed more than 5 years prior to initial assignment or in which there has been a break in service or employment in excess of 1 year subsequent to completion of the investigation, a reinvestigation is required.

C3.5.5.1.2.3.3. Subsequent to initial assignment to the PRP, reinvestigation is not required so long as the individual remains in the PRP.

C3.5.5.1.2.3.4. A medical evaluation of the individual as set forth in DoD Directive 5210.42 (reference (s)).

C3.5.5.1.2.3.5. Review of the individual's personnel file and other official records and information locally available concerning behavior or conduct which is relevant to PRP standards.

C3.5.5.1.2.3.6. A personal interview with the individual for the purpose of informing him of the significance of the assignment, reliability standards, the need for reliable performance, and of ascertaining his attitude with respect to the PRP.

C3.5.5.1.2.3.7. Service in the Army, Navy and Air Force Reserve does not constitute active service for PRP purposes.

C3.5.6. <u>Access to North Atlantic Treaty Organization (NATO) Classified Information</u>

C3.5.6.1. Personnel assigned to a NATO staff position requiring access to NATO COSMIC (TOP SECRET), SECRET or CONFIDENTIAL information shall have

been the: subject of a favorably adjudicated BI (10-year scope), DNACI/NACI or NACI ENTNAC, current within five years prior to the assignment, in accordance with USSAN Instruction 1-69 (reference (kk)) and paragraph C3.7.6., below.

C3.5.6.2. Personnel not assigned to a NATO staff position, but requiring access to NATO COSMIC, SECRET or in the normal course of their duties, must possess the equivalent final U.S. security clearance based upon the appropriate personnel security investigation (Appendix 1) required by paragraphs C3.4.2. and C3.7.10. of this Regulation.

C3.5.7. Other Special Acces Programs(SAPs). Special investigative requirements for SAPs not provided for in this paragraph may be established only as part of the written program approval of the Deputy Secretary of Defense in accordance with the SAP approval process prescribed for in DoD Directive O-5205.7 (reference (qq)).

C3.6. CERTAIN POSITIONS NOT NECESSARILY REQUIRING ACCESS TO CLASSIFIED INFORMATION

C3.6.1. General. DoD Directive 5200.8 (reference (t)) outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of property or places under their command. Essential to carrying out this responsibility is a commander's need to protect the command against the action of untrustworthy persons. Normally, the investigative requirements prescribed in this Regulation should suffice to enable a commander to determine the trustworthiness of individuals whose duties require access to classified information or appointment to positions that are sensitive and do not involve such access. However, there are certain categories of positions or duties which, although not requiring access to classified information, if performed by unworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security. The investigative requirements for such positions or duties are detailed in this section.

C3.6.2. Access to Restricted Areas, Sensitive Information or Equipment Not Involving Access to Classified Information

C3.6.2.1. Access to restricted areas, sensitive information or equipment by DoD military, civilian or contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or ENTNAC) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate DoD Component Agency or activity prior to permitting such access. DoD Components shall not request, and shall not direct or permit their contractors to

request, security clearances to permit access to areas when access to classified information is not required in the normal course of duties or which should be precluded by appropriate security measures. In determining trustworthiness under this paragraph, the provisions of paragraph C2.2.1. and Appendix 8 will be utilized.

C3.6.2.2. In meeting the requirements of this paragraph, approval shall be obtained from one of the authorities designated in paragraph AP5.1., Appendix 5 of this Regulation, for authority to request NACs on DoD military, civilian or contractor employees. A justification shall accompany each request which shall detail the reasons why escorted access would not better serve the national security. Requests for investigative requirements beyond a NAC shall be forwarded to the Deputy Under Secretary of Defense for Policy for approval.

C3.6.2.3. NAC requests shall:

C3.6.2.3.1. Be forwarded to DIS in accordance with the provisions of paragraph AP2.2., Appendix 2,

C3.6.2.3.2. Contain a reference to this paragraph on the DD Form 398-2, and

C3.6.2.3.3. List the authority in Appendix 5 who approved the request.

C3.6.2.4. Determinations to deny access under the provisions of this paragraph must not be exercised in an arbitrary, capricious, or discriminatory manner and shall be the responsibility of the military or installation commander as provided for in DoD Directive 5200.8 (reference (t)).

C3.6.3. Nonappropriated Fund Employees. Each Nonappropriated Fund employee who is employed in a position of trust as designated by an official authorized in paragraph AP5.9., Appendix 5, shall have been the subject of a NAC completed no longer than 12 months prior to employment or a prior personnel security investigation with no break in Federal service or employment greater than 12 months in accordance with DoD 1401.1-M, (reference (u)). An individual who does not meet established suitability requirements may not be employed without prior approval of the authorizing official. Issuance of a CONFEDENTIAL or SECRET clearance will be based on a DNACI or NACI in accordance with paragraph C3.4.2.

C3.6.4. Customs Inspectors. DoD employees appointed as customs inspectors, under waivers approved in accordance with DoD 5030.49-R (reference (v)), shall have undergone a favorably adjudicated NAC completed within the past 5 years unless there has been a break in DoD employment greater than 1 year in which case a current NAC is

required.

C3.6.5. Red Cross/United Service Organizations Personnel (USO). A favorably adjudicated NAC shall be accomplished on Red Cross or United Service Organizations personnel as prerequisite for assignment with the Armed Forces overseas (DoD Directive 5210.25 (reference (w))).

C3.6.6. Officials Authorized to Issue Security Clearance. Any person authorized to adjudicate personnel security clearances shall have been the subject of a favorably adjudicated BI.

C3.6.7. Personnel Security Clearance adjudication Officials. Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated BI.

C3.6.8. Persons Requiring DoD Building Passes. Pursuant to DoD Directive 5210.46 (reference (z)), each person determined by the designated authorities of the DoD Components concerned as having an official need for access to DoD buildings in the National Capital Region shall be the subject of a favorably adjudicated NAC prior to issuance of a DoD building pass. Conduct of a BI for this purpose is prohibited unless approved in advance by ODUSD(P).

C3.6.9. Foreign National Employees Overseas Not Requiring Access to Classified Information. Foreign nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of the following record checks, initiated by the appropriate Military Department investigative organization consistent with paragraph C2.4.5., prior to employment:

C3.6.9.1. Host-government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and

C3.6.9.2. DCII;

C3.6.9.3. FBI-HQ/ID (where information exists regarding residence by the foreign national in the United States for one year or more since age 18).

C3.6.10. Special Agents and Investigative Support Personnel. Special agents and those noninvestigative personnel assigned to investigative agencies whose official duties require continuous access to complete investigative files and material require an SBI.

C3.6.11. Persons Requiring Access to Chemical Agents. Personnel whose duties involve access to or security of chemical agents shall be screened initially for suitability and reliability and shall be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required. At a minimum, all such personnel shall have had a favorably adjudicated NAC completed within the last 5 years prior to assignment in accordance with the provisions of DoD Directive 5210.65 (reference (y)).

C3.6.12. Education and Orientation Personnel. Persons selected for duties in connection with programs involving the education and orientation of military personnel shall have been the subject of a favorably adjudicated NAC prior to such assignment. This does not include teachers/administrators associated with university extension courses conducted on military installations in the United States. Non-US citizens from a country listed in Appendix 8 shall be required to undergo a BI if they are employed in a position covered by this paragraph.

C3.6.13. Contract Guards. Any person performing contract guard functions shall have been the subject of a favorably adjudicated NAC prior to such assignment.

C3.6.14. Transportation of Arms, Ammunition and Explosives (AA&E). Any DoD military, civilian or contract employee (including commercial carrier) operating a vehicle or providing security to a vehicle @porting Category I, II or CONFIDENTIAL AA&E shall have been the subject of a favorably adjudicated NAC or ENTNAC.

C3.6.15. Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II and ADP-III. DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with Appendix 10) and investigated as follows:

ADP-I:	BI
ADP-II:	DNACI/NACI
ADP-III:	NAC/ENTNAC

Those personnel falling in the above categories who require access to classified information will, of course, be subject to the appropriate investigative scope contained in paragraph C3.4.2., above.

C3.6.16. Others. Requests for approval to conduct an investigation on other personnel, not provided for in paragraphs C3.6.2. through C3.6.14., above, considered to fall with the general provisions of paragraph C3.6.1., above, shall be submitted, detailing the justification therefor, for approval to the Deputy Under Secretary of Defense for

Policy. Approval of such requests shall be contingent upon an assurance that appropriate review procedures exist and that adverse determinations will be made at no lower than major command level.

C3.7. REINVESTIGATION

C3.7.1. General. DoD policy prohibits unauthorized and unnecessary investigations. There are, however, certain situations and requirements that necessitate reinvestigation of an individual who has already been investigated under the provisions of this regulation. It is the policy to limit reinvestigation of individuals to the scope contained in paragraph AP1.1.1.4., Appendix 1, to meet overall security requirements. Reinvestigation, generally, is authorized only as follows:

C3.7.1.1. To prove or disprove an allegation relating to the criteria set forth in paragraph C2.2.1. of this Regulation with respect to an individual holding a security clearance or assigned to a position that requires a unworthiness determination;

C3.7.1.2. To meet the periodic reinvestigation requirements of this Regulation with respect to those security programs enumerated below; and

C3.7.1.3. Upon individual request, to assess the current eligibility of individuals who did not receive favorable adjudicative action after an initial investigation, if a potential clearance need exists and there are reasonable indications that the factors upon which the adverse determination was made no longer exists.

C3.7.2. Allegations Related to Disqualification. Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the disqualification criteria outlined in paragraph C2.2.1. that could have an adverse impact on an individual's security status, a Special Investigative Inquiry (SII), psychiatric, drug or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative subject, and the subject fails to furnish the required data, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with paragraph C8.2.2. of this Regulation.

C3.7.3. Access to Sensitive Compartmented Information (SCI). Each individual having current access to SCI shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.7.4. Critical-sensitive Positions. Each DoD civilian employee occupying a critical sensitive position shall be the subject of a PR conducted an a 5-year recurring,

basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.7.5. Presidential Support Duties. Each individual assigned Presidential Support duties shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.7.6. NATO Staff. Each individual assigned to a NATO staff position requiring a COSMIC clearance shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1. Those assigned to a NATO staff position requiring a NATO SECRET clearance shall be the subject of a new NAC conducted on a 5-year recurring basis.

C3.7.7. Extraordinarily Sensitive Duties. In extremely limited instances, extraordinary national security implications associated with certain SCI duties may require very special comparanentation and other special security measures. In such instances, a Component SOIC may, with the approval of the Deputy Under Secretary of Defense for Policy, request PRs at intervals of less than 5 years as outlined in paragraph AP1.1.1.4., Appendix 1. Such requests shall include full justification and a recommendation as to the desired frequency. In reviewing such requests, the Deputy Under Secretary of Defense for Policy shall give due consideration to:

C3.7.7.1. The potential damage that might result from the individuals defection or abduction.

C3.7.7.2. The availability and probable effectiveness of means other than reinvestigation to evaluate factors concerning the individual's suitability for continued SCI access.

C3.7.8. Foreign Nationals Employed by DoD Organizations Overseas. Foreign nationals employed by DoD organizations overseas who have been granted a "Limited Access Authorization" shall be the subject of a PR, as set forth in paragraph AP1.1.1.4., Appendix 1, conducted under the auspices of DIS by the appropriate Military Department or other U.S. Government investigative agency consistent with paragraph C2.4.5. and Appendix 9 of this Regulation.

C3.7.9. Persons Accessing Very Sensitive Information Classified Secret

C3.7.9.1. Heads of DoD Components shall submit a request to the Deputy Under Secretary of Defense for Policy for approval to conduct periodic reinvestigations on persons holding Secret clearances who are exposed to very sensitive Secret information.

C3.7.9..2. Generally, the Deputy Under Secretary of Defense for Policy will only approve periodic reinvestigations of persons having access to Secret information if the unauthorized disclosure of the information in question could reasonably be expected to:

C3.7.9.2.1. Jeopardize human life or safety.

C3.7.9.2.2. Result in the loss of unique or uniquely productive intelligence sources or methods vital to the United States security.

C3.7.9.2.3. Compromise technologies, plans, or procedures vital to the strategic advantage of the United States.

C3.7.9.3. Each individual accessing very sensitive Secret information who has been designated by an authority listed in paragraph AP5.1., Appendix 5 as requiring periodic reinvestigation, shall be the subject of a PR conducted on a 5-year recurring basis scoped as stated in paragraph AP1.1.1.4., Appendix 1.

C3.7.10. Access Top Secret Information. Each individual having current access to Top Secret information shall be the subject of a PR conducted on a 5-year recurring basis scoped as outlined in paragraph AP1.1.1.4., Appendix 1.

C3.7.11. Personnel Occupying Computer Positions Designated ADP-I. All DoD military, civilians, consultants, and contractor personnel occupying computer positions designated ADP-I, shall be the subject of a PR conducted on a 5-year recurring basis as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.8. AUTHORITY TO WAIVE INVESTIGATIVE REQUIRENMNTS

C3.8.1. Authorized Officials. Only an official designated in paragraph AP5.7., Appendix 5, is empowered to waive the investigative requirements for appointment to a sensitive position, assignment to sensitive duties or access to classified information pending completion of the investigation required by this chapter. Such waiver shall be based upon certification in writing by the designated official that such action is necessary to the accomplishment of a DoD mission. A minor investigative element that has not been met should not preclude favorable adjudication--nor should this require a waiver when all other information developed on an individual during the course of a prescribed investigation is favorable.

C4. CHAPTER 4

RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

C4.1. RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

C4.1.1. General. Investigations conducted by DoD organizations or another Agency of the Federal Government shall not be duplicated when those investigations meet the scope and standards for the level of the clearance or access required. The DoD Components that grant access (SCI or SAP) or issue security clearances (TOP SECRET, SECRET, and CONFIDENTIAL) to civilian and/or military or contractor employees are responsible for determining whether such individuals have been previously cleared or investigated by the U.S. Government. Any previously granted security clearance or access, which is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance or access required, shall provide the basis for issuance of a new clearance and/or access without further investigation or adjudication. Previously conducted investigations and previously rendered personnel security determinations shall be accepted within the Department of Defense, in accordance with the policy in sections C4.1.2. through C4.1.4. below.

C4.1.2. Prior Personnel Security Investigations. As long as there is no break in Military Service and/or Federal employment greater than 24 months, any previous personnel security investigation that essentially is equivalent in scope to an investigation required by this Regulation will be accepted without requesting additional investigation. There is no time limitation as to the acceptability of such investigations, subject to the provisions of paragraphs C2.3.8. and C4.1.3.2. of this Regulation.

C4.1.3. Prior Personnel Security Determinations Made by DoD Authorities

C4.1.3.1. Adjudicative determinations for appointment in sensitive positions, assignment to sensitive duties or access to classified information (including those pertaining to SCI) made by designated DoD authorities will be mutually and reciprocally accepted by all DoD Components without requiring additional investigation, unless there has been a break in the individual's Military Service and/or Federal employment of greater than 24 months or unless derogatory information that occurred subsequent to the last prior security determination becomes known. A check of the DCII or other appropriate databases should be conducted to accomplish this task.

C4.1.3.2. Whenever a valid DoD security clearance or access eligibility is on record, Components shall not request DIS or other DoD investigative organizations to forward prior investigative files for review unless:

C4.1.3.2.1. Significant derogatory information or investigation completed subsequent to the date of last clearance and/or an access authorization, is known to the requester; or

C4.1.3.2.2. The individual concerned is being considered for a higher level clearance (e.g., Secret or Top Secret) or the individual does not have an access authorization and is being considered for one; or

C4.1.3.2.3. The most recent clearance or access authorization of the individual concerned was conditional or based on a waiver.

C4.1.3.3. Requests for prior investigative files authorized by this Regulation shall be made in writing, shall cite the specific justification for the request (i.e., upgrade of clearance, issue Special Access authorization, etc.), and shall include the date, level, and issuing organization of the individual's current or most recent security clearance or Special Access authorization.

C4.1.3.4. All requests for non-DoD investigative files, authorized under the criteria prescribed by paragraphs C4.1.3.1., C4.1.3.2.1., C4.1.3.2.2., C4.1.3.2.3., and C4.1.3.3., above, shall be:

C4.1.3.4.1. Submitted on DD Form 398-2 to DIS;

C4.1.3.4.2. Annotated as a "Single Agency Check" of whichever Agency developed the investigative file or to obtain the check of a single national agency.

C4.1.3.5. When further investigation is desired, in addition to an existing non-DoD investigative file, a DD Form 1879 will be submitted to DIS with the appropriate security forms attached. The submission of a Single Agency Check via DD Form 398-2 will be used to obtain an existing investigative file or check a single national agency.

C4.1.3.6. Whenever a civilian or military member transfers from one DoD activity to another, the losing organizations security office is responsible for advising the gaining organization of any pending action to suspend, deny or revoke the individual's security clearance as well as any adverse information that may exist in security, personnel or other files. In such instances the clearance shall not be reissued until the

questionable information has been adjudicated.

C4.1.4. Investigations Conducted and Clearances Granted by Other Agencies of the Federal Government

C4.1.4.1. Whenever a prior investigation or personnel security determination (including clearance for access to information classified under Executive Order 12356 (reference (j))) of another Agency of the Federal Government meets the investigative scope and standards of this Regulation, such investigation or clearance may be accepted for the investigative or clearance purposes of this Regulation, provided that the employment with the Federal Agency concerned has been continuous and there has been no break longer than 24 months since completion of the prior investigation, and further provided that inquiry with the Agency discloses no reason why the clearance should not be accepted. If it is determined that the prior investigation does not meet the provisions of this paragraph, supplemental investigation shall be requested.

C4.1.4.2. A NACI conducted by OPM shall be accepted and considered equivalent to a DNACI for the purposes of this Regulation.

C4.1.4.3. Department of Defense policy on reciprocal acceptance of clearances with the Nuclear Regulatory Commission and the Department of Energy is set for the in DoD Directive 5210.2 (reference (z)).

C5. CHAPTER 5

REQUESTING PERSONNEL SECURITY INVESTIGATIONS

C5.1. REQUESTING PERSONNEL SECURITY INVESTIGATIONS

C5.1.1. General. Requests for personnel security investigations shall be limited to those required to accomplish the Defense mission. Such requests shall be submitted only by the authorities designated in paragraph C5.1.2., below. These authorities shall be held responsible for determining if persons under their jurisdiction require a personnel security investigation. Proper planning must be effected to ensure that investigative requests are submitted sufficiently in advance to allow completion of the investigation before the time it is needed to grant the required clearance or otherwise make the necessary personnel security determination.

C5.1.2. Authorized Requesters. Requests for personnel security investigation shall be accepted only from the requesters designated below:

C5.1.2.1. Military Departments

C5.1.2.1.1. Army

C5.1.2.1.1.1. Central Clearance Facility.

C5.1.2.1.1.2. All activity commanders.

C5.1.2.1.1.3. Chiefs of recruiting stations.

C5.1.2.1.2. Navy (including Marine Corps)

C5.1.2.1.2.1. Central Adjudicative Facility.

C5.1.2..1.2.2. Commanders and commanding officers of organizations listed on the Standard Navy Distribution List.

C5.1.2.1.2.3. Chiefs of recruiting stations.

C5.1.2.1.3. Air Force

C5.1.2.1.3.1. Air Force Security Clearance Office.

C5.1.2.1.3.2. Assistant Chief of Staff for Intelligence.

C5.1.2.1.3.3. All activity commanders.

C5.1.2.1.3.4. Chiefs of recruiting stations.

C5.1.2.2. Defense Agencies--Directors of Security and activity commanders.

C5.1.2.3. Organization of the Joint Chiefs of Staff--Chief, Security Division.

C5.1.2.4. Office of the Secretary of Defense--Director for Personnel and Security, Washington Headquarters Services.

C5.1.2.5. Commanders of the Combatant Commands or their designees.

C5.1.2.6. Such other requesters approved by the Deputy Under Secretary of Defense for Policy.

C5.1.3. Criteria for Requesting Investigations. Authorized requesters shall use the tables set forth in Appendix 3 to determine the type of investigation that shall be requested to meet the investigative requirement of the specific position or duty concerned.

C5.1.4. Request Procedures. To insure efficient and effective completion of required investigations, all requests for personnel security investigations shall be prepared and forwarded in accordance with Appendix 2 and the investigative jurisdictional policies set forth in section C2.4. of this Regulation.

C5.1.5. Priority Requests. To insure that personnel security investigations are conducted in an orderly and efficient manner, requests for priority for individual investigations or categories of investigations shall be kept to a minimum. DIS shall not assign priority to any personnel security investigation or categories of investigations without written approval of the Deputy Under Secretary of Defense for Policy.

C5.1.6. Personal Data Provided by the Subject of the Investigation

C5.1.6.1. To conduct the required investigation, it is necessary that the investigative agency be provided certain relevant data concerning the subject of the investigation. The Privacy Act of 1974 (reference (m)) requires that, to the greatest extent practicable, personal information shall be obtained directly from the subject individual when the information may result in adverse determinations affecting an individual's rights, benefits, and privileges under Federal programs.

C5.1.6.2. Accordingly, it is incumbent upon the subject of each personnel security investigation to provide the personal information required by this Regulation. At a minimum, the individual shall complete the appropriate investigative forms, provide fingerprints of a quality acceptable to the FBI, and execute a signed release, as necessary, authorizing custodians of police, credit, education, employment, and medical and similar records, to provide relevant record information to the investigative agency. When the FBI returns a fingerprint card indicating that the quality of the fingerprints is not acceptable, an additional set of fingerprints wail be obtained from the subject. In the event the FBI indicates that the additional fingerprints are also unacceptable, no further attempt to obtain more fingerprints need be made; this aspect of the investigation will then be processed on the basis of the name check of the FBI files. As an exception, a minimum of three attempts will be made (1) for all Presidential Support cases, (2) for SCI access nominations if the requester so indicates, and (3) in those cases in which more than minor derogatory information exists. Each subject of a personnel security investigation conducted under the provisions of this regulation shall be furnished a Privacy Act Statement advising of (1) the authority for obtaining the personal data, (2) the principal purpose(s) for obtaining it, (3) the routine uses, (4) whether disclosure is mandatory or voluntary, (5) the effect on the individual if it is not provided, and (6) that subsequent use of the data may be employed as part of an a periodic review process to evaluate continued eligibility for access to classified information.

C5.1.6.3. Failure to respond within the time limit prescribed by the requesting organization with the required security forms or refusal to provide or permit access to the relevant information required by this Regulation shall result in termination of the individual's security clearance or assignment to sensitive duties utilizing the procedures of paragraph C8.2.2. or further administrative processing of the investigative request.

C6. CHAPTER 6

ADJUDICATION

C6.1. ADJUDICATION

C6.1.1. General

C6.1.1.1. The standard that must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

C6.1.1.2. The principal objective of the DoD personnel security adjudicative function, consequently, is to assure selection of persons for sensitive positions who meet this standard. The adjudication process involves the effort to assess the probability of future behavior, which could have an effect adverse to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. It is invariably a subjective determination, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.

C6.1.1.3. Establishing relevancy is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. It involves neither the judgment of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a person's trustworthiness and fitness for a responsibility that could, if abused, have unacceptable consequences for the national security.

C6.1.1.4. While equity demands optimal uniformity in evaluating individual cases, assuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts, and prior experience in similar cases. All information of record, both

favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness,and overall significance. In all adjudications the protection of the national security shall be the paramount determinant.

C6.1.2. Central Adjudication

C6.1.2.1. To ensure uniform application of the requirement of this Regulation and to ensure that DoD personnel security determinations are effected consistent with existing statutes and Executive orders, the Head of each Military Department and Defense Agencies shall establish a single Central Adjudication Facility for his/her component. The function of such facility shall be limited to evaluating personnel security investigations and making personnel security determinations. The chief of each Central Adjudication Facility shall have the authority to act on behalf of the Head of the Component concerned with respect to personnel security determinations. All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this Regulation shall be reviewed and evaluated by personnel security specialists specifically designated by the Head of the Component concerned, or designee.

C6.1.2.2. In view of the significance each adjudicative decision can have on a person's career and to ensure the maximum degree of fairness and equity in such actions, a minimum level of review shall be required for all clearance/access determinations related to the following categories of investigations:

C6.1.2.2.1. BI/SBI/PR/ENAC/SII:

C6.1.2.2.1.1. Favorable: Completely favorable investigations shall be reviewed and approved by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3.

C6.1.2.2.1.2. Unfavorable: Investigations that are not completely favorable shall undergo at least two levels of review by adjudicative officials, the second of which must be at the civilian grade of GS-11/12 or the military rank of O-4. When an unfavorable administrative action is contemplated under paragraph C8.2.2., the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS-13/14 or the military rank of O-5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS-14/15 or the military rank of O-6.

C6.1.2.2.2. NACI/DNACI/NAC/ENTNAC:

C6.1.2.2.2.1. Favorable: A completely favorable investigation may be finally adjudicated after one level of review provided that the decision making authority is at the civilian grade of GS-5/7 or the military rank of O-2.

C6.1.2.2.2.2. Unfavorable: Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3. When an unfavorable administrative action is contemplated under paragraph C8.2.2., the letter of intent to deny/ revoke must be signed by an adjudicative official at the civilian grade of GS-11/12 or the military rank of O-4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS-13 or the military rank of O-5 or above.

C6.1.2.2.3. Exceptions to the above policy may only be granted by the Deputy Under Secretary of Defense for Policy.

C6.1.3. Evaluation of Personnel Security Information

C6.1.3.1. The criteria and adjudicative policy to be used in applying the principles at paragraph C6.1.1., above, are set forth in paragraph C2.2.1. and Appendix 8 of this Regulation. The ultimate consideration in making a favorable personnel security determination is whether such determination is clearly consistent with the interests of national security and shall be an overall common sense evaluation based on all available information. Such a determination shall include consideration of the following factors:

C6.1.3.1.1. The nature and seriousness of the conduct;

C6.1.3.1.2. The circumstances surrounding the conduct;

C6.1.3.1.3. The frequency and recency of the conduct;

C6.1.3.1.4. The age of the individual;

C6.1.3.1.5. The voluntariness of participation; and

C6.1.3.1.6. The absence or presence of rehabilitation.

C6.1.3.2. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in Appendix 8. Adjudication policy for access to SCI is contained in DCID 1/14.

C6.1.4. Adjudicative Record

C6.1.4.1. Each adjudicative determination, whether favorable or unfavorable, shall be entered into the Defense Clearance and Investigations Index (DCII) on a daily basis but in no case to exceed 5-working days from the date of determination.

C6.1.4..2. The rationale underlying each unfavorable personnel security determination to include the appeal process, and each favorable personnel security determination where the investigation or information upon which the determination was made included significant derogatory information of the type set forth in paragraph C2.2.1. and Appendix 8 of this Regulation shall be maintained in written or automated form and is subject to the provisions of DoD Directives 5400.7 (reference (aa)) and 5400.11 (reference (bb)). This information shall be maintained for aminimum of 5 years from the date of determination.

C7. CHAPTER 7

ISSUING CLEARANCE AND GRANTING ACCESS

C7.1. ISSUING CLEARANCE AND GRANTING ACCESS

C7.1.1. General

C7.1.1.1. The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subjects suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph C8.1.3.

C7.1.1.2. Only the authorities designated in paragraph AP5.1., Appendix 5 are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in paragraph C8.1.3. of this Regulation are complied with.

C7.1.1.3. All commanders and Heads of DoD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this Regulation.

C7.1.2. Issuing Clearance

C7.1.2.1. Authorities designated in paragraph AP5.1., Appendix 5 shall record the issuance, denial, or revocation of a personnel security clearance in the DCII (see paragraph C6.1.4., above). A record of the clearance issued shall also be recorded in an individual's personnel/security file or official personnel folder, as appropriate.

C7.1.2.2. A personnel security clearance remains valid until (1) the individual is separated from the Armed Forces, (2) separated from DoD civilian employment, (3)

has no further official relationship with the Department of Defense, (4) official action has been taken to deny, revoke or suspend the clearance or access, or (5) regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties. If an individual resumes the original status of (1), (2), (3), or (5) above, no single break in the individual's relationship with the Department of Defense exists greater than 24 months, and/or the need for regular access to classified information at or below the previous level recurs, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

C7.1.2.3. Personnel security clearances of DoD military personnel shall be granted, denied, or revoked only by the designated authority of the parent Military Department. Issuance, reissuance, denial, or revocation of a personnel security clearance by any DoD Component concerning personnel who have been determined to be eligible for clearance by another component is expressly prohibited. Investigations conducted on Army, Navy, and Air Force personnel by DIS will be returned only to the parent Service of the subject for adjudication regardless of the source of the original request. The adjudicative authority will be responsible for expeditiously transmitting the results of the clearance determination. As an exception, the employing DoD Component may issue an interim clearance to personnel under their administrative jurisdiction pending a final eligibility determination by the individual's parent DoD Component. Whenever an employing DoD Component issues an interim clearance to an individual from another DoD Component, written notice of the action shall be provided to the parent DoD Component.

C7.1.2.4. When an SSBI (or PR) for access to SCI is initiated on a military member, who is assigned to a Defense Agency (except DIA), OSD staff, or the Joint Staff, DIS will return the completed investigation to the appropriate Military Department CAF, in accordance with subsection C7.1.2.3., above, for issuance (or reissuance) of the SCI eligibility. The CAF shall be responsible for expeditiously transmitting the results of the SCI eligibility determination to the requesting Defense Agency. For military personnel assigned to the DIA, the completed investigation will be forwarded to the DIA for the SCI eligibility determination. The DIA will expeditiously transmit the results of the SCI eligibility determination to the appropriate Military Department CAF.

C7.1.2.5. When the Defense Industrial Security Clearance Office (DISCO) initiates an SSBI (or PR) for access to SCI on a contractor employee, DIS will return the completed investigation to the appropriate CAF with SCI cognizance. Following a favorable SCI eligibility determination, the CAF will notify DISCO of the outcome. If the SCI eligibility is denied or revoked, the CAF will complete all appropriate due

process and appeal procedures before forwarding the case and all relevant additional documentation to DISCO for appropriate action, to include referral to the Defense Office of Hearings and Appeals (DOHA) for possible action under DoD Directive 5220.6 (reference (c)).

C7.1.2.6. The interim clearance shall be recorded in the DCII (paragraph C6.1.4., above) by the parent DoD Component in the same manner as a final clearance.

C7.1.3. Granting Access

C7.1.3.1. Access to classified information shall be granted to persons whose official duties require such access and who have the appropriate personnel security clearance. Access determinations (other than for Special Access programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

C7.1.3.2. In the absence of derogatory information on the individual concerned, DoD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DoD authority authorized by this Regulation to issue personnel security clearance, as the basis for granting access, when access is required, without requesting additional investigation or investigative files.

C7.1.3.3. The access level of cleared individuals will, wherever possible, be entered into the Defense Clearance and Investigations Index (DCII), along with clearance eligibility. However, completion of the DCII Access field is required effective October 1, 1993, in all instances where the adjudicator is reasonably aware of the level of classified access associated with a personnel security investigation. Agencies are encouraged to start completing this field as soon as possible.

C8. CHAPTER 8

UNFAVORABLE ADMINISTRATIVE ACTIONS

C8.1. REQUIREMENTS

C8.1.1. General. For purposes of this Regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at paragraph DL1.1.2., and any unfavorable personnel security determination, as defined at paragraph DL1.1.29. This chapter is intended only to provide guidance for the internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

C8.1.2. Referral for Action

C8.1.2.1. Whenever derogatory information related to the criteria and policy set forth in paragraph C2.2.1. and Appendix 8 of this Regulation is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall insure that the appropriate Central Adjudicative Facility (CAF) of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto. However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the CAF to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph C8.2.2., below, if such action is warranted and supportable by the criteria and policy contained in paragraph C2.2.1. and Appendix 8. No unfavorable administrative action as defined in paragraphs DL1.1.28. and DL1.1.29. may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in paragraph C8.2.2., below, or, in the case of SCI, Annex B, DCID 1/14 (reference (l)).

C8.1.2.2. The Director DIS shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other

than through DoD command or industrial organization channels. Such access shall include utilization of the DoD Inspector General "hotline" to receive such reports for appropriate follow-up by DIS. DoD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DoD Components will augment the system when and where necessary. Heads of DoD Components will be notified immediately to take action if appropriate.

C8.1.3. Suspension.

C8.1.3.1. The commander or head of the organization shall determine whether, on the basis of all facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subjects security status unchanged or to take interim action to suspend subjects access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties (or other duties requiring a trustworthiness determination) until a final determination is made by the appropriate authority designated in Appendix 5.

C8.1.3.2. Whenever a determination is made to suspend a security clearance for access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), the individual concerned must be notified of the determination in writing by the commander, or component CAF, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.

C8.1.3.3. Component field elements must promptly report all suspension actions to the appropriate CAF, but not later than 10 working days from the date of the suspension action. The adjudicative authority will immediately update the DCII Eligibility and Access fields to alert all users to the individual's changed status.

C8.1.3.4. Every effort shall be made to resolve suspension cases as expeditiously as circumstances permit suspension cases exceeding 180 days shall be closely monitored and managed by the DoD Component concerned until finally resolved. Suspension cases pending in excess of 12 months will be reported to the DASD (I&S) for review and appropriate action.

C8.1.3.5. A final security clearance eligibility determination shall be made for all suspension actions and the determination entered in the DCII. If, however, the individual under suspension leaves the jurisdiction of the Department of Defense and no longer requires a clearance (or trustworthiness determination), entry of the "Z" Code

(adjudication action incomplete due to loss of jurisdiction) in the clearance eligibility field is appropriate. In no case shall a "suspension" code (Code Y) remain a permanent record in the DCII

C8.1.3.6. A clearance or access entry in the DCII shall not be suspended or downgaded based solely on the fact that a periodic reinvestigation was not conducted precisely within the 5-year time period for TOP SECRET/SCI or within the period prevailing for SECRET clearances under departmental policy. While every effort should be made to ensure that PRs are conducted within the prescribed timeframe, agencies must be flexible in their administration of this aspect of the personnel security program so as not to undermine the ability of the Department of Defense to accomplish its mission.

C8.1.4. Final Unfavorable Administrative Actions. The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in Appendix 5, except that the authority to terminate the employment of a civilian employee of a Military Department or Defense Agency is vested solely in the head of the DoD Component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DoD Components, on the basis of criteria listed in paragraph C2.2.1., C2.2.1.1. through C2.2.1.6., shall be coordinated with the of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence OASD(C3I) prior to final action by the Head of the DoD Component. DoD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the Military Departments. However, actions contemplated in this regard shall not affect or limit the responsibility of the CAF to continue to process the individual for clearance, access to classified information, or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this Regulation.

C8.2. PROCEDURES

C8.2.1. General. No final unfavorable personnel security clearance or access determination shall be made on a Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in C8.2.2., below, when such determination results in an unfavorable administrative action (see paragraph C8.1.1.). As an exception, DoD contractor personnel shall be afforded the procedures contained in DoD Directive 5220.6 (reference (c)) and Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by DoD Directive 5210.25 (reference (w)). Procedures for to SAPs may differ from the procedures in this Regulation as authorized in E.O. 12968 and as approved by the Secretary of Defense or Deputy Secretary of Defense.

C8.2.2. Unfavorable Administrative Action Procedures. Except as provided for below, no unfavorable administrative action shall be taken under the authority of this Regulation unless the individual concerned has been:

C8.2.2.1. Provided a written statement of the reasons (SOR) as to why the unfavorable administrative action is being taken in accordance with the example at Appendix 11, which includes sample letters and enclosures. The SOR shall be as comprehensive and detailed as the protection of sources afforded confidentiality under provisions of the Privacy Act of 1974 (reference (m)) and national security permit. The statement will contain, 1) a summary of the security concerns and supporting adverse information, 2) instructions for responding to the SOR and 3) copies of the relevant security guidelines from Appendix 8. In addition, the CAF will provide within 30 calendar days, upon request of the individual, copies of releasable records of the personnel security investigation (the CAF must retain copies of the file for at least 90 days to ensure the ready availability of the material for the subject). If the CAF is unable to provide requested documents for reasons beyond their control, then the name and address of the Agency (Agencies) to which the individual may write to obtain a copy of the records will be provided.

C8.2.2.1.1. The head of the local organization of the individual receiving an SOR shall designate a point of contact (POC) to serve as a liaison between the CAF and the individual. The duties of the POC will include, but not necessarily be limited to, delivering the SOR, having the individual acknowledge receipt of the SOR; determining whether the individual intends to respond within the time specified; ensuring that the individual understands the consequences of the proposed action as well as the to respond in a timely fashion; explaining how to obtain time extensions, procure

copies of investigative records, and the procedures for responding to the SOR; and ensuring that the individual understands that he or she can obtain legal counsel or other assistance at his or her own expense.

C8.2.2.2. Afforded an opportunity to reply in writing to the CAF within 30 calendar days from the date to submit a timely response will result in forfeiture of all future appeal rights with regard to the unfavorable administrative action. Exceptions to this policy may only be circumstances where the individual's failure to respond to the SOR was due to factors beyond his or her control. The CAF must be notified of the individual's intent to respond, via the POC, within 10-calendar days of receipt of the SOR. An extension of up to 30-calendar days may be granted by the employing organization following submission of a written request from the individual. Additional extensions may only be granted by the CAF. Responses to the CAF must be forwarded through the head of the employing organization.

C8.2.2.3. Provided a written response by the CAF to any submission under subparagraph C8.2.2.2., above. stating the final reason(s) for the unfavorable administrative action, which shall be as specific as privacy and national security considerations permit and in accordance with the example of a letter of denial (IOD) and its enclosures at Appendix 11. Such response shall be as prompt as individual circumstances permit, not to exceed 60-calendar days from the date of receipt of the response submitted under subparagraph C8.2.2.2., above, provided no additional investigative action is necessary. If a final response cannot be completed within the time frame allowed, the individual must be notified in writing of this fact, the reasons therefor, and the date a final response is expected, which shall not normally exceed a total of 90 days from the date of receipt of the response under subparagraph C8.2.2.2.

C8.2.2.4. Afforded an opportunity to appeal an LOD, issued pursuant to paragraph C8.2.2.3., above to the DoD Component Personnel Security Appeals Board (PSAB). The PSAB shall consist of a minimum of three members and function in accordance with Appendix 12. If a decision is made to appeal the LOD, the individual may do so by one of the following methods:

C8.2.2.4.1. Appeal Without a Personal Appearance: Advise the PSAB within 10-calendar days of receipt of the LOD, of the intent to appeal. Within 40-calendar days of receipt of the LOD, write to the appropriate PSAB stating reasons why the LOD should be overturned and providing any additional, relevant information that may have a bearing on the final decision by the PSAB;

C8.2.2.4.2. Appeal With a Personal Appearance: Advise the Defense Office of Hearings and Appeals (DOHA) within 10-calendar days of receipt of the LOD

that a personal appearance before a DOHA Administrative Judge (AJ) is desired in order to provide additional, relevant information, which may have a bearing on the final decision by the PSAB. DOHA will promptly schedule a personal appearance and will provide a recommendation to the PSAB generally within 60 days of receipt of the requesting the personal appearance. Procedures governing the conduct of the personal appearance before a DOHA AJ are contained at Appendix 13.

C8.2.2.5. Provided a final written decision by the PSAB, including a rationale, to any submission under subparagraph C8.2.2.4., above, stating the final disposition of the appeal. This will nominally be accomplished within 60-calendar days of receipt of the written appeal from the individual if no personal appearance was requested, or within 30-calendar days from receipt of the AJ's recommendation if a personal appearance was requested.

C8.2.3. Due Process Review. The due process and appeal procedures will be reviewed one year after implementation. The above procedures will become effective no later than 120 days after the date of this change.

C8.2.4. Exceptions to Policy. Notwithstanding paragraph C8.2.2., above or any other provision of this Regulation, nothing in this Regulation shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to Section 7532, Title 5, United States Code (reference (pp)). Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph C8.2.2., above, are not appropriate. Such determination shall be conclusive.

C8.3. REINSTATEMENT OF CIVILIAN EMPLOYEES

C8.3.1. General. Any person whose civilian employment in the Department of Defense is terminated under the provisions of this Regulation shall not be reinstated or restored to duty or reemployed in the Departmentof Defense unless the Secretary of Defense, or the Head of a DoD Component, finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of national security. Such a finding shall be made part of the personnel security record.

C8.3.2. Reinstatement Benefits. A DoD civilian employee whose employment has been suspended or terminated under the provisions of this Regulation and who is reinstated or restored to duty under the provisions of Section 3571 of Title 5, U.S.

Code (reference (dd)) is entitled to benefits as provided for by Section 3 of Public Law 89-380 (reference (ee)).

C9. CHAPTER 9

CONTINUING SECURITY RESPONSIBILITIES

C9.1. EVALUATING CONTINUED SECURITY ELIGIBILITY

C9.1.1. General. A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood-of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty that any human being will remain trustworthy. Accordingly, the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to assure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself. Therefore, the Heads of DoD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process.

C9.1.2. Management Responsibility

C9.1.2.1. Commanders and heads of organizations shall insure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this Regulation) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.

C9.1.2..2. The Heads of all DoD Components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long term, job-related security problems.

C9.1.3. Supervisory Responsibility. Security programs shall be established to

insure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should be disseminated concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the individual concerned to correct any personal problem which may have a bearing upon the individuals continued eligibility for access.

C9.1.3.1. In conjunction with the submission of PRs stated in Section C3.7., Chapter 3, and paragraph AP1.1.1.4., Appendix 1, supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's continued eligibility for access to classified information is omitted.

C9.1.3.2. If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package.

"I am aware of no information of the type contained at Appendix 5, DoD 5200.2-R, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information."

C9.1.3.3. If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package:

"I am aware of information of the type contained in Appendix E, DoD 5200.2-R, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s)."

C9.1.3.4. In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs

C9.1.3.2. and C9.1.3.3., above, as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.

C9.1.4. Individual Responsibility

C9.1.4.1. Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust in this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

C9.1.4.2. Moreover, individuals having access to classified information must report promptly to their security office:

C9.1.4.2.1. Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

C9.1.4.2.1.1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

C9.1.4.2.1.2. The employee is concerned that he or she may be the target of exploitation by a foreign entity.

C9.1.4.2.2. Any information of the type referred to in paragraph C2.2.1. or Appendix 8.

C9.1.5. Coworker Responsibility. Coworkers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information employed in a sensitive position.

C9.2. SECURITY EDUCATION

C9.2.1. General. The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DoD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DoD personnel security program. Accordingly, Heads of

DoD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

C9.2.2. Initial Briefings

C9.2.2.1. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this Regulation shall be given an initial security briefing. The briefing shall be in accordance with the requirements of paragraph 10-102., DoD 5200.1-R (reference (q)) and consist of the following elements:

C9.2.2.1.1. The specific security requirements of their particular job.

C9.2.2.1.2. The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

C9.2.2.1.3. The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

C9.2.2.1.4. The penalties that may be imposed for security violations.

C9.2.2.2. If an individual declines to execute Standard Form 312, "Classified Information Nondisclosure Agreement" (replaced the Standard Form 189). the DoD Component shall initiate action to deny or revoke the security clearance of such person in accordance with paragraph C8.1.3., above.

C9.2.3. Refresher Briefing. Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10-101. DoD 5200.1-R (reference (q)) shall be tailored to fit the needs of the experienced personnel.

C9.2.4. Foreign Travel Briefing. While world events during the past several years have diminished the threat to our national security from traditional cold-war era foreign intelligence services, foreign intelligence services continue to pursue the unauthorized acquisition of classified or otherwise sensitive U.S. Government information, through the recruitment of U.S. Government employees with access to such information. Through security briefings and education, the Department of Defense continues to provide for the protection of information and technology considered vital to the national security interests from illegal or unauthorized acquisition by foreign intelligence

services.

C9.2.4.1. DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security office all contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities in which:

C9.2.4.1.1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

C9.2.4.1.2. The employee is concerned that he or she may be the target of exploitation by a foreign entity.

C9.2.4.2. The DoD security manager, security specialist, or other qualified individual will review and evaluate the reported information. Any facts or circumstances of a reported contact with a foreign national that appear to:

C9.2.4.2.1. Indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive, or classified Information or technology,

C9.2.4.2.2. Offer a reasonable potential for such, or

C9.2.4.2.3. Indicate the possibility of continued contact with the foreign national for such purposes, shall be promptly reported to the appropriate counterintelligence agency.

C9.2.5. Termination Briefing

C9.2.5.1. Upon termination of employment administrative withdrawal of security clearance or contemplated absence from duty or employment for 60 days or more DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

C9.2.5.1.1. An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD Regulations applicable to the safeguarding of classified information to which the individual has had access and understands the implications thereof.

C9.2.5.1.2. A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

C9.2.5.1.3. An acknowledgment that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

C9.2.5.1.4. An acknowledgment that the individual will report without delay to the FBI or DoD Component concerned any attempt by any unauthorized person to solicit classified information.

C9.2.5.2. When an Individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service, who shall ensure that it is recorded in the Defense Clearance and Investigations Index.

C9.2.5.3. The Security Termination Statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's records retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

C9.2.5.4. In addition to the provisions of subparagraphs C9.2.5.1., C9.2.5.2., and C9.2.5.3., above, DoD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers and GS-16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy.

C10. CHAPTER 10

SAFEGUARDING PERSONNEL SECURITY INESTIGATIVE RECORDS

C10.1. SAFEGUARDING PERSONNEL SECURITY INESTIGATIVE RECORDS

C10.1.1. General. In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information shall be handled with the highest degree of discretion. Access to such information shall be afforded only for the purpose cited herein and to persons whose official duties require such information. Personnel security investigative reports may be used only for the purposes of determining eligibility of DoD military and civilian personnel, contractor employees, and other persons affiliated with the Department of Defense, for access to classified information, assignment or retention in sensitive duties or other specifically designated duties requiring such investigation, or for law enforcement and counterintelligence investigations. Other uses are subject to the specific written authorization of the Deputy Under Secretary of Defense for Policy.

C10.1.2. Responsibilities. DoD authorities responsible for administering the DoD personnel security program and all DoD personnel authorized access to personnel security reports and records shall ensure that the use of such information is limited to that authorized by this Regulation and that such reports and records are safeguarded as prescribed herein. The Heads of DoD Components and the Deputy Under Secretary of Defense for Policy for the Office of the Secretary of Defense shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records as required by paragraph C10.1.3. and C10.1.4., below.

C10.1.3. Access Restrictions. Access to personnel security investigative reports and personnel security clearance determination information shall be authorized only in accordance with DoD Directives 5400.7 and 5400.11 (references (aa) and (bb)) and with the following:

C10.1.3.1. DoD personnel security investigative reports shall be released outside of the Department of Defense only with the specific approval of the investigative agency having authority over the control and disposition of the reports.

C10.1.3.2. Within the Department of Defense, access to personnel security investigative reports shall be limited to those designated DoD officials who require access in connection with specifically assigned personnel security duties, or other

activities specifically identified under the provisions of paragraph C10.1.1., above.

C10.1.3.3. Access by subjects of personnel security investigative reports shall be afforded in accordance with DoD Directive 5400.11 (reference (bb)).

C10.1.3.4. Access to personnel security clearance determination information shall be made available, other than provided for in C10.1.3.3., above, through security channels, only to the Department of Defense or other officials of the Federal Government who have an official need for such information.

C10.1.4. Safeguarding Procedures. Personnel security investigative reports and personnel security determination information shall be safeguarded as follows:

C10.1.4.1. Authorized requesters shall control and maintain accountability of all reports of investigation received.

C10.1.4.2. Reproduction, in whole or in part, of personnel security investigative reports by requesters shall be restricted to the minimum number of copies required for the performance of assigned duties.

C10.1.4.3. Personnel security investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lock or and an approved three-position dial-type combination padlock or in a similarly protected area/container.

C10.1.4.4. Reports of DoD personnel security investigations shall be sealed in double envelopes or covers when transmitted by mail or when carried by persons not authorized access to such information. The inner cover shall bear a notation substantially as follows:

C10.1.4.5. An individual's status with respect to a personnel security clearance or a Special Access authorization is to be protected as provided for in paragraph 6.3.6., DoD Directive 5400.7 (reference (aa)).

C10.1.5. Records Disposition

C10.1.5.1. Personnel security investigative reports, to include OPM NACIs may be retained by DoD recipient organizations, only for the period necessary to complete the purpose for which it was originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization. All copies of such reports shall be destroyed within 90 days after completion of the required personnel security determination. Destruction shall be accomplished in the same manner as for classified information in accordance with

paragraph 9-101., DoD 5200.1-R (reference (q)).

C10.1.5.2. DoD record repositories authorized to file personnel security investigative reports shall destroy PSI reports of a favorable or of a minor the completion date of the investigation or the date on which the record was last released to an authorized user--whichever is later. Personnel security investigative reports resulting in an unfavorable administrative personnel action or court-martial or other investigations of a significant nature due to information contained the investigation shall be destroyed 25 years after the date of the last action. Files in this latter category that are determined to be of possible historical value and those of widespread public or congressional interest may be offered to the National Archives after 15 years.

C10.1.5.3. Personnel security investigative reports on persons who are considered for affiliation with the Department of Defense will be destroyed after 1 year if the affiliation is not completed.

C10.1.6. Foreign Source Information. Information that is classified by a foreign government is exempt from public disclosure under the Freedom of Information and Privacy Acts. Further, information provided by foreign governments requesting an express promise of confidentiality shall be released only in a-manner that will not identify or allow unauthorized persons to identify the foreign agency concerned.

C11. CHAPTER 11

PROGRAM MANAGEMENT

C11.1. PROGRAM MANAGEMENT

C11.1.1. General. To ensure uniform implementation of the DoD personnel security program throughout the Department, program responsibility shall be centralized at the DoD Component level.

C11.1.2. Responsibilities

C11.1.2.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) shall have primary responsibility for providing guidance, oversight, development and approval for policy and procedures governing personnel security program matters within the Department:

C11.1.2.1.1. Provide program management through isuance of policy and operating guidance.

C11.1.2.1.2. Provide staff assistance to the DoD Components and Defense Agencies in resolving day-to-day security policy and operating problems.

C11.1.2.1.3. Conduct inspections of the DoD Components for implementation and compliance with DoD security policy and operating procedures.

C11.1.2.1.4. Provide policy, oversight, and guidance to the Component adjudication functions.

C11.1.2.1.5. Approve, coordinate and oversee all DoD personnel security research initiatives and activities.

C11.1.2.2. The General Counsel shall ensure that the program is administered in a manner consistent with the laws; all proceedings are promptly initiated and expeditiously completed; and that the rights of individuals involved are protected, consistent with the Interests of national security. The General Counsel shall also ensure that all relevant decisions of the courts and legislative initiatives of the Congress are obtained on a continuing basis and that analysis of the foregoing is accomplished and disseminated to DoD personnel security program management authorities.

C11.1.2.3. The Heads of the CoDComponents shall ensure that:

C11.1.2.3.1. The DoD personnel security program is administered within their area of responsibility in a manner consistent with this Regulation.

C11.1.2.3.2. A single authority within the office of the Head of the DoD Component is assigned responsibility for administering the program within the Component.

C11.1.2..3.3. Information and recommendations are provided the ASD(C3I) and the General Counsel at their request concerning any aspect of the program.

C11.1.3. Reporting Requirements

C11.1.3.1. The OASD(C3I) shall be provided personnel security program management data by the Defense Data Manpower Center (DMDC) by 31 December each year for the preceding fiscal year. To facilitate accurate preparation of this report, all adjudicative determinations must be entered into the DCII by all DoD central adjudication facilities no later than the end of the fiscal year. The information required below is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and Congress. The report shall cover the preceding fiscal year, broken out by clearance category, according to military (officer or enlisted), civilian or contractor status and by the central adjudication facility that took the action, using the enclosed format:

C11.1.3..1.1. Number of Top Secret, Secret, and Confidential clearances issued;

C11.1.3.1.2. Number of Top Secret, Secret, and Confidential clearances denied;

C11.1.3.1.3. Number of Top Secret, Secret, and Confidential clearances revoked;

C11.1.3.1.4. Number of SCI access determinations issued;

C11.1.3.1.5. Number of SCI access determinations denied;

C11.1.3.1.6. Number of SCI access determinations revoked; and

C11.1.3.1.7. Total number of personnel holding a clearance for Top Secret, Secret, Confidential, and Sensitive Compartmented Information as of the end of the fiscal year.

C11.1.3.2. The Defense Investigative Service (DIS) shall provide the OASD(C3I) a quarterly report that reflects investigative cases opened and closed during the most recent quarter by case category type, and by major requester. The information provided by DIS is essential for evaluating statistical data regarding investigative workload and the manpower required to perform personnel security investigations. Case category types include National Agency Checks (NACs); Expanded NACS; Single Scope Background Investigations; Periodic Reinvestigations (PRs); SECRET Periodic Reinvestigations (SPRs); Post Adjudicative; Special Investigative Inquiries (SlIs); and Limited Inquiries. This report shall be forwarded to OASD(C3I) within 45 days after the end of each quarter.

C11.1.3.3. The reporting requirement for DMDC and DIS has been assigned Report Control Symbol DD-C31(A)1749.

C11.1.4. Inspections. The Heads of DoD Components shall assure that personnel security program matters are included in their administrative inspection programs.

C12. CHAPTER 12

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)

C12.1. DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)

C12.1.1. General

C12.1.1.1. The Defense Clearance and Investigations Index (DCII) is the single, automated central repository that identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities.

C12.1.1.2. The DCII database consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained, by subject, in the DCII.

C12.1.1.3. DoD investigative and adjudicative authorities report information which is used for investigative, adjudicative, statistical, research and other purposes as authorized by OASD(C3I) approval.

C12.1.2. Access. The DCII is operated and maintained by the Defense Investigative Service (DIS). Access is nominally limited to the Department of Defense and other Federal Agencies with adjudicative, investigative, and/or counterintelligence (CI) missions. Agencies wishing to gain access to the DCII must submit a written request outlining specific requirements with corresponding justification, as stated in paragraph C12.1.2.1. through C12.1.2.4., below. On approval, a Memorandum of Understanding (MOU) addressing equipment, maintenance, security, privacy, and other Agency responsibilities shall be forwarded to the requester by DIS for signature.

C12.1.2.1. Military Departments. Requests from Military Departments or organizations must be submitted for approval and endorsement through the following offices to DIS, Director, National Computer Center, P.O. Box 1211, Baltimore, MD 21203-1211.

C12.1.2.1.1. Air Force. Administrative Assistant to the Secretary of the Air Force, Pentagon, Room 4D881, Washington, DC 20330-4000.

C12.1.2.1.2. Army. Director, Counterintelligence and Security Countermeasures, Office of the Deputy Chief of Staff for Intelligence, Department of the Army, Pentagon, Room 2D481, Washington, DC 20301-1050.

C12.1.2.1.3. Navy and Marine Corps. Director, Information and Personnel Security Policy Directorate, Naval Criminal Investigative Service, Chief of Naval Operations (OP-09N), Washington, DC 20350-2000.

C12.1.2.2. Combatant Commands. Requests from Combatant Commands must be submitted for approval to DIS, Director, National Computer Center through the Joint Chiefs of Staff, Chief, Security Division, Directorate for Information and Resource Management, The Joint Staff, Room 1B738, The Pentagon, Washington, DC 20318-9300.

C12.1.2.3. Defense Agencies. Requests from DoD Agencies must be submitted through, and with the approval of, the Agency's Security Headquarters Office to DIS, Director, National Computer Center, P.O. Box 1211, Baltimore, MD 21203-1211.

C12.1.2.4. Non-DoD Agencies. Requests from Non-DoD Agencies must be submitted to the Deputy Assistant Secretary of Defense (Intelligence and Security), Attn: Counterintelligence and Security Programs, Room 3C281, 6000 Defense Pentagon, Washington, DC 20301-6000. On approval, those requests shall be forwarded to the DIS for action.

C12.1.3. Investigative Data. Contributors to the DCII shall ensure that all investigative data on an individual is entered into the DCII.

C12.1.3.1. An entry shall be made to indicate a pending investigation when an investigation is opened.

C12.1.3.2. When an investigation has been completed, the contributor shall change the DCII status to reflect a completed investigation, including the date (year) of the investigation.

C12.1.3.3. Changes or additions to existing files must, whenever appropriate, all be reflected in the DCII.

C12.1.3.4. Investigative file tracings may be deleted from the DCII when the retention period is over and the record file has been destroyed.

C12.1.4. Adjudicative Data. All adjudicative determinations on personnel with access to classified information or performing sensitive duties shall be indexed in the DCII.

C12.1.4.1. Specifically, a DCII clearance entry shall be created or updated as follows:

C12.1.4.1.1. Immediately upon suspension of access.

C12.1.4.1.2. When interim access has been authorized by the CAF or employing activity.

C12.1.4.1.3. Immediately following the granting, denial, or revocation of a clearance or access.

C12.1.4.1.4. Following the receipt, review, and adjudication of information received subsequent to the prior clearance or access determination.

C12.1.4.2. DCII entries shall inform the DoD Components of the clearance eligibility and/or access status of an individual or the presence of an adjudicative file.

C12.1.4.3. An adjudicative determination shall remain in the DCII as long as the subject is affiliated with the Department of Defense. The determination may be deleted 2 years after the employment and/or clearance eligibility ends. The deleted DCII data shall be retained by the DIS in a historical file for a minimum of 5 years after deletion by the contributor.

C12.1.4.4. The date of the DCII clearance and/or access entry shall always be the same as or subsequent to the date of the most recent investigation.

C12.1.4.5. DoD Components will notify the CAF of applicable personnel changes to ensure the accuracy of the DCII database.

C12.1.5. Notification to Other Contributors. Whenever a DoD contributor to the DCII becomes aware of significant unfavorable information about an individual with a clearance and/or access entry from another DoD contributor, immediate notification must be made to the latter along with copies of all relevant information.

C12.1.6. Security Requirements for the DCII

C12.1.6.1. The DCII is an unclassified system that meets the C-2 level of

protection under the Computer Security Act of 1987. Contributors may enter only unclassified information.

C12.1.6.2. Information contained in the DCII receives the protection required by the Privacy Act of 1974 (reference (m)).

C12.1.6.2.1. Due to the sensitive nature of the information, positions having direct (password) access to a DCII terminal are considered to be ADP-1 Critical Sensitive Positions.

C12.1.6.2.2. Individuals authorized access to the DCII must have a favorably completed SSBI (or BI and/or SBI).

C12.1.6.2.3. DoD activities and other Federal Agencies that have been authorized "Read Only" access to the DCII must also comply with those investigative requirements.

C12.1.6.3. Each authorized contributor is responsible for the accuracy of the data it enters. Contributors may enter, modify or delete only data originated by them. The DCII shall not allow one contributor to alter or delete another contributor's information.

C12.1.6.4. To prevent unauthorized access or tampering during nonworking hours, DCII terminals must be located in an area that is secured by guard personnel, an alarm system, or appropriate locking device.

C12.1.6.5. When the DCII terminal is operational, access to DCII information shall be controlled and limited to those persons authorized access to that information.

C12.1.7. Disclosure of Information. The Privacy Act of 1974 requires an accounting of the disclosure of personal information when it is provided to another Agency. For accessing the DCII, the Department of Defense is considered a single Agency. Disclosure of personal information in the Department of Defense does not require specific accounting for each disclosure. All releases of information obtained from the DCII to any non-DoD source must be recorded in the DCII Disclosure Accounting System (DDAS) by the Agency that releases the information. A contributor may disclose only the DCII data originated by that contributor to the subject of the data. Requests for release of investigative reports or adjudicative files are handled as Privacy Act requests by contributors.

AP1. APPENDIX 1

INVESTIGATIVE SCOPE

AP1.1.1. This appendix prescribes the scope of the various types of personnel security investigations.

AP1.1.1.1. National Agency Check. The scope for NAC is five years or to age 18, whichever is the shorter period. At a minimum, the first three of the described Agencies (DCII, FBLIHQ, and FBI/ID), below, shall be included in each complete NAC; however, a NAC may also include a check of any or all of the other described Agencies, if appropriate.

AP1.1.1.1.1. The DCII database consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained, by subject, in the DCII. DCII records will be checked on all subjects of DoD investigations.

AP1.1.1.1.2. FBI/HQ has on file copies of investigations conducted by the FBI. The FBI/HQ check, included in every NAC, consists of a review of files for information of a security nature and that developed during applicant-type investigations.

AP1.1.1.1.3. An FBI/ID check, included in every NAC (but not ENTNAC), is based upon a technical fingerprint search that consists of a classification the subject's fingerprints and comparison with fingerprint cards submitted by law enforcement activities. If the fingerprint card is not classifiable, a "name check only" of these files is automatically conducted.

AP1.1.1.1.4. OPM. The files of OPM contain the results of investigations conducted by OPM under E.O. 9835 and 10450 (references (ff) and (g)), those requested by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE), and those requested since August 1952 to serve as a basis for "Q" clearances. OPM records are checked on all persons who are, or who have been, civilian employees of the U.S. Government; or U.S. citizens who are, or who have been, employed by a United Nations organization or other public international organization; and on those who have been granted security clearances by the NRC or the DOE.

AP1.1.1.1.5. Immigration and Naturalization Service (I&NS). The files

of I&NS contain (or show where filed) naturalization certificates, certificates of derivative citizenship, all military certificates of naturalization, repatriation files, petitions for naturalization and declaration of intention, visitors' visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the U.S. I&NS records are checked when the subject is:

AP1.1.1.1.5.1. An alien in the United States, or

AP1.1.1.1.5.2. A naturalized citizen whose naturalization has not been verified, or

AP1.1.1.1.5.3. An immigrant alien, or

AP1.1.1.1.5.4. A U.S. citizen who receives derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

AP1.1.1.1.6. State Department. The State Department maintains the following records:

AP1.1.1.1.6.1. Security Division (S/D) files contain information pertinent to matters of security, violations of security, personnel investigations pertinent to that agency, and correspondence files from 1950 to date. These files are checked on all former State Department employees.

AP1.1.1.1.6.2. Passport Division (P/D) shall be checked if subject indicates U.S. citizenship due to birth in a foreign country of American parents. This is a check of State Department Embassy files to determine if subject's birth was registered at the U.S. Embassy in the country where he was born. Verification of this registration is verification of citizenship.

AP1.1.1.1.7. Central Intelligence Agency (CIA). The CIA maintains the following records:

AP1.1.1.1.7.1. Directorate of Operations (CIA-DO/IMS) maintains the Foreign Intelligence/Counterintelligence database. This database shall be checked for all aliens residing outside the United States requiring access to classified information (i.e., LAA). If the requester provides complete personal identifying information (Complete Name, Date of Birth, Place of Birth, and Citizenship), all alien co-subjects (on SSBIS) residing outside the United States are also checked. In addition, this database shall be queried on the Subject any time there is a counterintelligence

concern raised during the conduct of the personnel security investigation.

AP1.1.1.1.7.2. Office of Security (CIA-SEC) maintains information on present and former employees, including members of the Office of Strategic Services (OSS), and applicants for employment. These files shall be checked if subject has been an employee of the CIA or when other sources indicate that CIA may have pertinent information.

AP1.1.1.1.8. Military Personnel Record Center files are maintained by separate Departments of the Armed Forces, General Services Administration and the Reserve Records Centers. They consist of the Master Personnel Records of retired, separated, Reserve, and active duty members of the Armed Forces. These records shall be checked when the requester provides required identifying data indicating service during the last 5 years.

AP1.1.1.1.9. Treasury Department. The files of Treasury Department Agencies (Secret Service, Internal Revenue Service, and Bureau of Customs) will be checked only when available information indicates that an Agency of the Treasury Department may be reasonably expected to have pertinent information.

AP1.1.1.1.10. The files of other Agencies, such as the National Guard Bureau, the Defense Industrial Security Clearance Office (DISCO), etc., will be checked when pertinent to the purpose for which the investigation is being conducted.

AP1.1.1.2. Single Scope Background Investigation (SSBI): The following SSBI scope reflects the requirements of National Security Directive 63 (reference (rr)).

AP1.1.1.2.1. Scope: The period of investigation for an SSBI is the last ten (10) years or to age 18, whichever is the shorter period, provided that the investigation covers at least the last 2 full years of the subject's life. No investigation will be conducted for the period prior to an individual's 16th birthday. Emphasis shall be placed on peer coverage whenever interviews are held with personal sources in making education, employment, and reference (including developed) contact.

AP1.1.1.2.2. Expansion of Investigation. The investigation may be expanded as necessary, to resolve issues and/or address employment standards unique to individual agencies.

AP1.1.1.2.3. NAC. Checks on subject and spouse/cohabitant of investigative and criminal history files of the Federal Bureau of Investigation, including submission of fingerprint records on the subject, and such other national Agencies

(DCII, INS, OPM, CIA, etc.). In addition to conducting a NAC on the subject of the investigation, the following additional requirements apply.

AP1.1.1.2.3.1. A DCII, FBLID name check only and FBI/HQ check shall be conducted on subject's spouse or cohabitant. In addition, such other national agency checks as deemed appropriate based on information on the subject's PSQ shall be conducted.

AP1.1.1.2.3.2. A check of FBI/HQ files on members of subject's immediate family who are 18 years of age or older and who are non-U.S. citizens shall be conducted. As used throughout the Regulation, members of subject's immediate family include the following:

AP1.1.1.2.3.2.1. Current spouse.

AP1.1.1.2.3.2.2. Adult children, 18 years of age or older, by birth, adoption, or marriage.

AP1.1.1.2.3.2.3. Natural, adopted, foster, or stepparents.

AP1.1.1.2.3.2.4. Guardians.

AP1.1.1.2.3.2.5. Brothers and sisters either by birth, adoption, or remarriage of either parent.

AP1.1.1.2.3.2.6. Cohabitant.

AP1.1.1.2.3.3. The files of CIA shall be reviewed on non-U.S. citizens of subject's immediate family who are 18 years of age or older.

AP1.1.1.2.3.4. I&NS files on members of subject's immediate family 18 years of age or older shall be reviewed when they are:

AP1.1.1.2.3.4.1. Non-U.S. citizens, or

AP1.1.1.2.3.4.2. Naturalized U.S. citizens whose naturalization has not been verified in a prior investigation, or

AP1.1.1.2.3.4.3. U.S. citizens born in a foreign country of American parent(s) or U.S. citizens who received derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

AP1.1.1.2.4. Subject Interview. Required in all cases and shall be conducted by trained security, investigative, or counterintelligence personnel to ensure full investigative coverage. An additional personal interview shall be conducted when necessary to resolve any significant information and/or inconsistencies developed during the investigation. In Departments or Agencies with policies sanctioning the use of polygraph for personnel security purposes, the personal interview may include a polygraph examination, conducted by a qualified polygraph examiner;

AP1.1.1.2.5. Birth. Independent certification of date and place of birth received directly from appropriate registration authority if not otherwise verified under A1.1.1.2.6., below, or if a variance is developed.

AP1.1.1.2.6. Citizenship. Subject must be a U.S. citizen. Independent verification of citizenship received directly from appropriate registration authority. For foreign-born immediate family members 18 years of age or older, verification of citizenship or, legal status is also required. Subject's citizenship status must be verified in all cases. U.S. citizens who are subjects of investigation will be required to produce documentation that will confirm their citizenship. Normally such documentation should be presented to the DoD Component concerned prior to the initiation of the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that the designated authority in the DoD Component will be provided with the documentation prior to the issuance of a clearance. DIS will not check the BVS for native-born U.S. citizens except as indicated in AP1.1.1.2.5., above. In the case of foreign-born U.S. citizens, DIS will check I&NS records. The citizenship status of all foreign-born members of subject's immediate family shall be verified. Additionally, when the investigation indicates that a member of subject's immediate family has not obtained

U.S. citizenship after having been eligible for a considerable period of time, an attempt should be made to determine the reason. The documents listed below are acceptable for proof of U.S. citizenship for personnel security determination purposes:

AP1.1.1.2.6.1. A birth certificate must be presented if the individual was born in the United States. To be acceptable, the certificate must show that the birth record was filed shortly after birth and must be certified with the registrar's signature and the raised, impressed, or multicolored seal of his office except for States or jurisdictions which, as a matter of policy, do not issue certificates with a raised or impressed seal. Uncertified copies of birth certificates are not acceptable.

AP1.1.1.2.6.1.1. A delayed birth certificate (a record filed more than one year after the date of birth) is acceptable provided that it shows that the report of birth was supported by acceptable secondary evidence of birth as described in subparagraph A1.1.1.2.6.1.2., below.

AP1.1.1.2.6.1.2. If such primary evidence is not obtainable, a notice from the registrar stating that no birth record exists should be submitted. The notice shall be accompanied by the best combination of secondary evidence obtainable. Such evidence may include a baptismal certificate, a certificate of circumcision, a hospital birth record, affidavits of persons having personal knowledge of the facts of the birth, or other documentary evidence such as early census, school, or family bible records, newspaper files and insurance papers. Secondary evidence should have been created as close to the time of birth as possible.

AP1.1.1.2.6.1.3. All documents submitted as evidence of birth in the United States shall be original or certified documents. Uncertified copies are not acceptable.

AP1.1.1.2.6.2. A certificate of naturalization shall be submitted if the individual claims citizenship by naturalization.

AP1.1.1.2.6.3. A certificate of citizenship issued by the I&NS shall be submitted if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

AP1.1.1.2.6.4. A "Report of Birth Abroad of A Citizen of The United States of American" (Form FS-240), a "Certification of Birth" (Form FS-545 or DS-1350), or a "Certificate of Citizenship" is acceptable if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

AP1.1.1.2.6.5. A passport or one in which the individual was included

will be accepted as proof of citizenship.

AP1.1.1.2.7. Education: Independent verification of most recent or most significant claimed attendance and/or degree/diploma within the scope of investigation via sealed transcript received directly from the institution. If all education is outside of the investigative scope, the last education above high school level will be verified.

AP1.1.1.2.8. Employment: Direct verification through records of all periods of employment within scope but in any event the most recent two (2) years. Personal interviews of two sources (supervisor/coworkers) for each employment of six months or more shall be attempted. In the event that no employment exceeds six months, interviews of supervisor/coworkers shall be attempted. All periods of unemployment in excess of sixty (60) days shall be verified through records and/or sources. All prior Federal/Military service and type of discharge(s) shall be verified.

AP1.1.1.2.8.1. Non-Federal Employment. Verify all employment within the period of investigation to include seasonal, holiday, Christmas, part-time, and temporary employment. Interview one supervisor and one coworker at subject's current place of employment as well as at each prior place of employment during the past 10 years of six months duration or longer. The interview requirement for supervisors and coworkers does not apply to seasonal, holiday, Christmas, part-time, and temporary employment (4 months or less) unless there are unfavorable issues to resolve or the letter of inquiry provides insufficient information.

AP1.1.1.2.8.2. Federal Employment. All Federal employment will be verified within the period of investigation to include Christmas, seasonal temporary, summer hire, part-time, and holiday employment. Do not verify Federal employment through review of records if already verified by the requester. If Federal employment has not been verified by the requester, then subject's personnel file at his/her current place of employment will be reviewed. All previous Federal employment will be verified during this review. In the case of former Federal employees, records shall be examined at the Federal Records Center in St. Louis, Missouri. Interview one supervisor and one coworker at all places of employment during the past 10 years if so employed for 6 months or more.

AP1.1.1.2.8.3. Military Employment. Military service for the last 10 years shall be verified. The subject's duty station, for the purpose of interview coverage, is considered as a place of employment. One supervisor and one coworker shall be interviewed at subject's current duty station if subject has been stationed there for 6 months or more; additionally, a supervisor and a co-worker at subject's prior duty stations where assigned for 6 months or more during the past 5 years shall be

interviewed. Do not verify military employment through review of local records if already verified by the requester.

AP1.1.1.2.8.4. Unemployment. Subject's activities during all periods of unemployment in excess of 60 consecutive days, within the period of investigation, that are not otherwise accounted for shall be determined.

AP1.1.1.2.8.5. When an individual has resided outside the United States continuously for over one year, attempts will be made to confirm overseas employments as well as conduct required interviews of a supervisor and co-worker.

AP1.1.1.2.9. References: Four required (at least three of which are developed). To the extent practical, all should have social knowledge of subject and collectively span the entire scope of the investigation. As appropriate, additional interviews may include cohabitants(s), ex-spouses, and relative(s). Interviews with psychological/medical personnel are to be accomplished as required to resolve issues. Three developed character references who have sufficient knowledge of subject to comment on his background, suitability, and loyalty shall be interviewed. Efforts shall be made to interview developed references whose combined association with subject covers the full period of the investigation with particular emphasis on the last 5 years. Employment, education, and neighborhood references, in addition to the required ones, may be used as developed references provided that they have personal knowledge concerning the individual's character, discretion, and loyalty. A listed character reference will be interviewed only when developed references are not available or when it is necessary to identify and locate additional developed character references or when it is necessary to verify subject's activities (e.g., unemployment).

AP1.1.1.2.10. Neighborhood: Interviews with neighbors for the last five years if residence exceeds six months. Confirmation of current residence shall be accomplished regardless of length to include review of rental records if necessary. In the event no residence exceeds six months, interview of neighbors should be undertaken at current residence. During each neighborhood investigation, interview two neighbors who can verify subject's period of residence in that area and who were sufficiently acquainted to comment on subject's suitability for a position of trust. Neighborhood investigations will be expanded beyond this 5-year period only when there is unfavorable information to resolve in the investigation. Neighborhood investigations are not required outside the United States and Puerto Rico.

AP1.1.1.2.11. Credit: Verification of the subject s financial status and credit habits at all locations where subject has resided, been employed, or attended school for six months or more for the last seven (7) years. Conduct credit bureau

check in the 50 States, the District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided) at all places where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months or more, on a cumulative basis, during the last 7 years or during the period of the investigation, whichever is shorter. Financial responsibility, including unexplained affluence, will be stressed in all reference interviews.

AP1.1.1.2.12. Local Agency Checks: A check of appropriate police records, including state central criminal history record repositories, covering all locations where subject has resided, been employed, or attended school for six months or more during the scope of investigation, to include current residence regardless of duration. In the event that no residence, employment, or education exceeds six months, local agency checks should be conducted at the current residence, current employment, and last educational institution attended.

AP1.1.1.2.13. Foreign Travel. If subject has been employed, educated, traveled or resided outside of the United States for more than 90 days during the period of investigation, except under the auspices of the U.S. Government, additional record checks during the NAC shall be made in accordance with paragraph A1.1.1.2.6.of this Appendix. In addition, the following requirements apply:

AP1.1.1.2.13.1. Foreign travel not under the auspices of the U.S. Government. When employment education, or residence has occurred overseas for more than 90 days during the past 10 years or since age 18, which was not under the auspices of the U.S. Government, a check of records will be made at the Passport Office of the Department of State and other appropriate Agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas to cover significant employment, education, or residence and to determine whether the individual has worked or lived outside of the United States continuously for over one year, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

AP1.1.1.2.13.2. Foreign travel under the auspices of the U.S. Government. When employment, education, or residence has occurred overseas for a period of more than one year, under the auspices of the U.S. Government, a record check will be made at the Passport Office of the Department of State and other appropriate Agencies. Efforts shall be made to develop sources (generally in the United States) who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. Additionally, the investigation will be

expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

AP1.1.1.2.14. Foreign Connections. All foreign connections (friends, relatives, and/or business connections) of subject and immediate family in the United States or abroad, except where such association was the direct result of subject's official duties with the U.S. Government, shall be ascertained. Investigation shall be directed toward determining the significance of foreign connections of the part of subject and the immediate family, particularly where the association is or has been with persons whose origin was within a country whose national interests are inimical to those of the United States

AP1.1.1.2.15. Organizations. Efforts will be made during reference interviews and record reviews to determine if subject and/or the immediate family has, or formerly had, membership in, affiliation with, sympathetic association towards, or participated in any foreign or domestic organization, association, movement, group, or combination of persons of the type described in paragraphs C2.2.1.1. through C2.2.1.4. of this Regulation.

AP1.1.1.2.16. Military Service. All Military Service and types of discharge during the last 10 years shall be verified.

AP1.1.1.2.17. Medical Records. Medical records shall not be reviewed unless:

AP1.1.1.2.17.1. The requester indicates that subject's medical records were unavailable for review prior to submitting the request for investigation, or

AP1.1.1.2.17.2. The requester indicates that unfavorable information is contained in subject's medical records, or

AP1.1.1.2.17.3. The subject lists one or more of the following on the PSQ:

AP1.1.1.2.17.3.1. A history of mental or nervous disorders.

AP1.1.1.2.17.3.2. That subject is now or has been addicted to the use of habit-forming drugs such as narcotics or barbiturates or is now or has been a chronic user to excess of alcoholic beverages.

AP1.1.1.2.18. Public Records: Verification of divorce(s), bankruptcy,

etc., and any other court (civil or criminal) actions to which subject has been or is a party within the scope of investigation, when known or developed. Divorces, annulments, and legal separations of subject shall be verified only when there is reason to believe that the grounds for the action could reflect on subject's suitability for a position of trust.

AP1.1.1.2.19. Ex-spouse Interview. If the subject of investigation is divorced, the ex-spouse will be interviewed when the date of final divorce action is within the scope of investigation.

AP1.1.1.2.20. Polygraph: Agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary.

AP1.1.1.2.21. Select Scoping. When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

AP1.1.1.2.22. Transferability: Investigations satisfying the scope and standards specified above are transferable between Agencies and shall be deemed to meet the investigative standards for access to Collateral TOP SECRET/National Security Information and Sensitive Compartmented Information. No further investigation or reinvestigation prior to revalidation every five years will be undertaken unless the Agency has substantial information indicting that the transferring individual may not satisfy eligibility standards for clearance or the Agency head determines in writing that to accept the investigation would not be in the national security interest of the United States.

AP1.1.1.2.23. Updating a Previous Investigation to SSBI Standards. If a previous investigation does not substantially meet the minimum standards of an SSBI or if it is more than 5 years old, a current investigation is required but may be limited to that necessary to bring the individual's file up to date in accordance with the investigative requirements of an SSBI. Should new information be developed during the current investigation that bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

AP1.1.1.3. Periodic Reinvestigation (PR)

AP1.1.1.3.1. Each DoD military, civilian, consultant, and contractor employee occupying a critical sensitive position or possessing a TOP SECRET

clearance, or occupying a special access program position and non-U.S. citizens (foreign nationals and/or immigrant aliens) holding a limited access authorization shall be the subject of a PR initiated 5 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years.

AP1.1.1.3.2. Minimum Investigative Requirements. A PR shall include the following minimum scope.

AP1.1.1.3.2.1. NAC. A valid NAC on the SUBJECT will be conducted in all cases (NOTE: only a name check of the FBIJID will be conducted unless records indicate that a technical fingerprint check was not done previously). Checks of DCII, FBI/HQ, FBMD name check only, and other Agencies deemed appropriate, will be conducted on the Subject's current spouse or cohabitant, if not previously conducted. Additionally, NACs will be conducted on immediate family members, 18 years of age or older, who are non-U.S. citizens, if not previously accomplished.

AP1.1.1.3.2.2. Credit. Credit bureau checks covering all places where the SUBJECT resided for 6 months or more, on a cumulative basis, during the period of investigation, in the 50 States, District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided), will be conducted.

AP1.1.1.3.2.3. Subject Interview. The interview should cover the entire period of time since the last investigation, not just the last 5-year period. Significant information disclosed during the interview, which has been satisfactorily covered during a previous investigation, should not be explored again unless additional relevant information warrants further coverage.

AP1.1.1.3.2.4. Employment. Current employment will be verified. Military and Fderal service records will not routinely be checked, if previously checked by the requester when the PR was originally submitted. Also, employment records will be checked wherever employment interviews are conducted.

Records need be checked only when they are locally available, unless unfavorable information had been detected.

AP1.1.1.3.2.5. Employment References. Two supervisors or coworkers at the most recent place of employment or duty station of 6 months; if the current employment is less than 6 months employment reference interviews will be conducted at the next prior place of employment, which was at least a 6-month duration.

AP1.1.1.3.2.6. Developed Character References (DCRs). Two developed character references who are knowledgeable of the SUBJECT will be interviewed. Developed character references who were previously interviewed will only be reinterviewed when other developed references are not available.

AP1.1.1.3.2.7. Local Agency Checks (LACs). DIS will conduct local agency checks on the SUBJECT at all places of residence, employment, and education during the period of investigation, regardless of duration, including overseas locations (except overseas locations from which military members have transferred).

AP1.1.1.3.2.8. Neighborhood Investigation. Conduct a neighborhood investigation to verify subject's current residence in the United States. Two neighbors who can verify subject's period of residence in that area and who are sufficiently acquainted to comment on the subject's suitability for a position of trust will be interviewed. Neighborhood investigations will be expanded beyond the current residence when unfavorable information arises.

AP1.1.1.3.2.9. Ex-Spouse Interview. If the subject of investigation is divorced, the ex-spouse will be interviewed when the date of final divorce action is within the period of investigation.

AP1.1.1.3.2.10. Polygraph: Agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary.

AP1.1.1.3.2.11. Select Scoping. When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

AP1.1.1.4. Secret Periodic Reinvestigation (S-PR)

AP1.1.1.4.1. Each DoD military, civilian, consultant, and contractor employee with current access to SECRET information shall be the subject of a S-PR initiated 10 years from the date of completion of the last investigation. The PR shall

cover the period of the last 5 years.

AP1.1.1.4.2. Minimum Investigative Requirements. The S-PR shall include the following minimum scope.

AP1.1.1.4.2.1. NAC. A NAC with a name check of the FBI Identification Division, a check of the FBI Investigative Files, as well as other Agencies' indices, e.g., DoD, OPM, CIA, State, INS, etc., as appropriate. (NOTE: A technical fingerprint check of the FBI Identification Division will be conducted vice a name check if one was not done previously);

AP1.1.1.4.2.2. Credit. Conduct credit bureau checks at all locations where subject has resided, been employed, or attended an institution of higher Teaming for a period of six months or more during the period of coverage;

AP1.1.1.4.2.3. The investigation may be expanded as necessary to fully develop or resolve an issue.

AP2. APPENDIX 2

REQUEST PROCEDURES

AP2.1. GENERAL

To conserve investigative resources and to insure that personnel security investigations are limited to those essential to current operations and are clearly authorized by DoD policies, organizations requesting investigation must assure that continuing command attention is given to the investigative request process.

In this connection, it is particularly important that the provision of Executive Order 12356 (reference (j)) requiring strict limitations on the dissemination of official information and material be closely adhered to and limited to those that investigations requested for issuing clearances are instances in which an individual has a clear need for access to classified information. Similarly, investigations required to determine eligibility for appointment or retention in the Department of Defense, in either a civilian or military capacity, must not be requested in frequency or scope exceeding that provided for in this Regulation.

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

AP2.1.1. Limit requests for investigation to those-that are essential to current operations and clearly authorized by DoD policies and attempt to utilize individuals who, under the provisions of this Regulation, have already met the security standard;

AP2.1.2. Assure that military personnel on whom investigative requests are initiated will have sufficient time remaining in service after completion of the investigation to warrant conducting it;

AP2.1.3. Insure that request forms and prescribed documentation are properly executed in accordance with instructions;

AP2.1.4. Dispatch the request directly to the DIS Personnel Investigations Center;

AP2.1.5. Promptly notify the DIS Personnel Investigations Center if the investigation is no longer needed (notify OPM if a NACI is no longer needed); and

AP2.1.6. Limit access through strict need-to-know, thereby requiring fewer investigations.

In summary, close observance of the above-cited guidelines will allow the DIS to operate more efficiently and permit more effective, timely, and responsive service in accomplishing investigations.

AP2.2. NATIONAL AGENCY CHECK (NAC)

When a NAC is requested an original only of the DD Form 398-2 (National Agency Check Request) and a completed YD 258 (Applicant Fingerprint Card) are required. If the request is for an ENTNA.NC, an original only of the DD Form 398-2 and a completed DD Form 2280 (Armed Forces Fingerprint Card) are required. Those forms should be sent directly to:

Personnel Investigation Center
Defense Investigative Service
P.O. Box 1083
Baltimore, Maryland 21203

AP2.3. NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES (NACI)

When a NACI is requested, an original and one copy of the SF 85 (Data for Nonsensitive or Noncritical-sensitive Position), an SF 171 (Personal Qualifications Statement), and an SF 87 (U.S. Civil Service Commission Fingerprint Chart) shall be sent directly to:

Office of Personnel Management
Bureau of Personnel Investigations
NACI Center
Boyers, Pennsylvania 16018

The notation "ALL REFERENCES" shall be stamped immediately above the title at the top of the Standard Form 85.

AP2.4. DoD NATIONAL AGENCY CHECK WITH INQUIRIES (DNACI)

AP2.4.1. When a DNACI is requested, one copy of DD Form 1879, an original and two copies of the DD Form 398-2 (National Agency Check Request), two copies of FD 258 (Fingerprint Card), and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to:

Personnel Investigations Center
Defense Investigative Service
P.O. Box 1083
Baltimore, Maryland 21203

AP2.4.2. The DD Form 398-2 must be completed to cover the most recent five year period. All information, to include items relative to residences and employment, must be complete and accurate to avoid delays in processing.

AP2.5. SPECIAL BACKGROUND INVESTIGATION (SBI)/BACKGROUND INVESTIGATION (BI)

AP2.5.1. When requesting a BI or SBI, one copy of DD Form 1879 (Request for Personnel Security Investigation), an original and four copies of DD Form 398 (Statement of Personnel History), two copies of YD 258, and an original of DD Form 2221 Authority for Release of Information and Records) shall be sent directly to the:

Personnel Investigations Center
Defense Investigative Service
P.O. Box 454
Baltimore, Maryland 21203

AP2.5.2. For the BI and SBI, the DD Form 398 must be completed to cover the most recent five and 15 year period, respectively, or since the 18th birthday, which ever is shorter.

AP2.6. PERIODIC REINVESTIGATION (PR)

AP2.6.1. PRs shall be requested only in such cases as are authorized by paragraphs C3.7.1. through C3.7.11. of this Regulation.

AP2.6.1.1. For a PR requested in accordance with paragraph C3.7.1. and C3.7.11., the DD Form 1879 must be accompanied by the following documents:

AP2.6.1.1.1. Original and four copies of DD Form 398.

AP2.6.1.1.2. Two copies of FD-258.

AP2.6.1.1.3. Original copy of DD Form 2221

AP2.6.1.2. In processing PRs, previous investigative reports will not be requested by the requesting organization, unless significant derogatory or adverse information, postdating the most recent favorable adjudication, is developed during the course of reviewing other locally available records. In the latter instance, requests for previous investigative reports may only be made if it is determined by the requesting organization that the derogatory information is so significant that a review of previous investigative reports is necessary for current adjudicative determinations.

AP2.6.2. No abbreviated version of DD Form 398 may be submitted in connection with a PR.

AP2.6.3. The PR request shall be sent to the address in paragraph AP2.5.1., above.

AP2.7. ADDITIONAL INVESTIGATION TO RESOLVE DEROGATORY OR ADVERSE INFORMAITON

AP2.7.1. Requests for additional investigation-required to resolve derogatory or adverse information shall be submitted by DD Form 1879 (Request for Personnel Security Investigation) to the:

Defense Investigative Service
P.O. Box 454
Baltimore, Maryland 21203

Such requests shall set forth the basis for the additional investigation and describe the specific matter to be substantiated or disproved.

AP2.7.2. The request should be accompanied by an original and four copies of the DD Form 398, where appropriate, two copies of FD-258 and an original copy of DD Form 2221, unless such documentation was submitted within the last 12 months to DIS as part of a NAC or other personnel security investigation. If pertinent, the results of a

recently completed NAC, NACI, or other related investigative reports available should also accompany the request.

AP2.8. OBTAINING RESULTS OF PRIOR INVESTIGATIONS

Requesters requiring verification of a specified type of personnel security investigation, and/or requiring copies of prior investigations conducted by the DIS shall submit requests by letter or message to:

Defense Investigative Service Investigative Files Division
P.O. Box 1211
Baltimore, Maryland 21203

Message Address: DIS PIC BALTIMORE MD/ /D0640

The request will include subject's name, grade, social security number, date and place of birth, and DIS case control number, if known.

AP2.9. REQUESTING POST-ADJUDICATION

AP2.9.1. Requests pertaining to issues arising after adjudication of an investigation (post-adjudication cases) shall be addressed to DIS on a DD Form 1879 accompanied by a DD Form 398, where appropriate.

AP2.9.2. All requests for initial investigations will be submitted to PIC regardless of their urgency. If, however, there is an urgent need for a post-adjudication investigation, or the mailing of a request to PIC for initiation of a post-adjudication case would prejudice timely pursuit of investigative action, the DD Form 1879 may be directed for initiation, in CONUS, to the nearest DIS Field Office, and in overseas locations, to the military investigative service element supporting the requester (Appendix 9). The field element (either DIS or the military investigative agency) will subsequently forward either the DD Form 1879 or completed investigation to PIC.

AP2.9.3. A fully executed DD Form 1879 and appropriate supporting documents may not be immediately available. Further, a case that is based on sensitive security issues may be compromised by a request that the subject submit a DD Form 398. A brief explanation should appear on DD Form 1879s, which does not include complete supporting documentation.

AP2.10. REQUESTS INVOLVING CONTRACTOR EMPLOYEES

To preclude duplicative investigative requests and double handling of contractor employee cases involving access to classified information, all requests for investigation of contractor personnel must be submitted, using authorized industrial security clearance forms, for processing through the Defense Industrial Security Clearance Office, except for programs in which specific approval has been obtained from the Deputy Under Secretary of Defense for Policy to utilize other procedures.

AP2.11. RESPONSIBILITIES FOR PROPER DOCUMENTATION OF REQUESTS

The official signing the request for investigation shall be responsible for insuring that all documentation is completed in accordance with these instructions.

AP3. APPENDIX 3

TABLES FOR REQUESTING INVESTIGATIONS
GUIDE FOR REQUESTING BACKGROUND INVESTIGATIONS (BI)

TABLE 1

A	B	C
If the individual is a:	and duties require:	then a BI is required before:
U.S. national military member, civilian, consultant, or contractor employee	Top Secret clearance	granting final clearance
U.S. national civilian employee	assignment to a "Critical" sensitive position	assignment to the position
U.S. national military member, DoD civilian or contractor employee	occupying a "critical" position in the Nuclear Weapon Personnel Reliability Program (PRP) (reference (s))	occupying a "critical" position
U.S. national military member or civilian employee	granting, denying clearances	performing clearance functions
U.S. national military member or civilian employee	membership on security screening, hearing, or review board	appointment to the board
immigrant alien	limited access to Secret or Confidential information	issuing limited access authorization (Note 1)
non-U.S. national employee excluding immigrant alien	limited access to Secret or Confidential information	issuing limited access authorization
non-U.S. national employee for military education and orientation program (from a country listed at Appendix 7)	education and orientation of military personnel	before performing duties

NOTE 1 - will cover a 10-year scope.

TABLE 1 (continued)

If the individual is a:.	and duties require:	then a BI is required before:
U.S. national military member, DoD civilian or contractor employee	assignment to a category two Presidential Support position	assignment
U.S. national military member, DoD civilian or contractor employee assigned to NATO	access to NATO COSMIC information	access may be granted

TABLE 2
GUIDE FOR REQUESTING SPECIAL BACKGROUND INVESTIGATIONS (SBI)

A	B	C
If the individual is a:	and duties require:	then a SBI is required before:
U.S. national military member, DoD civilian, consultant, or contractor employee	access to SCI	granting access
	assignment to a category one Presidential Support position	assignment
	access to SIOP-ESI	granting access
	assignment to the National Security Agency	assignment
	access to other Special Access programs approved under paragraph C3.5.7.	granting access
	assignment to personnel security, counterintelligence, or criminal investigative or direct investigative support duties	assignment

TABLE 3
GUIDE FOR REQUESTING PERIODIC REINVESTIGATIONS (PR)

A	B	C
If the individual is a:	and duties require:	then a PR is required:
U.S. national military member, DoD civilian, consultant, or contractor employee	access to SCI	5 years from date of last SBI/BI or PR
	Top Secret Clearance	5 years from date of last SBI/BI or PR
	access to NATO COSMIC	5 years from date of last SBI/BI or PR
	assignment to Presidential Support activities	5 years from date of last SBI/BI or PR
U.S. national civilian employee	assignment to a "Critical" sensitive position	5 years from last SBI/BI or PR
Non-U.S. national employee	current limited access authorization to Secret or Confidential information	5 years from last SBI/BI or PR

TABLE 4
GUIDE FOR REQUESTING DoD NATIONAL AGENCY CHECK WITH INQUIRIES (DNACI) OR NACI

A	B	C
If the individual is a:	and duties require:	Then DNACI/NACI is required:
U.S. national military member or contractor employee	Secret clearance	before granting clearance (note 1)
	Interim Secret Clearance	may be automatically issued (note 2)
U.S. national civilian employee or consultant	Secret clearance	before granting clearance
	Interim Secret Clearance	may be automatically issued (note 3)
	Appointment to "Non Critical" sensitive position	before appointment
U.S. national military member, DoD civilian or contractor employee	occupying a "controlled" position in the Nuclear Weapon PRP (reference (s))	before assignment
applicant for appointment as a commissioned officer	commission in the Armed Forces	before appointment (after appointment for health professionals, chaplains, and attorneys, under conditions authorized by paragraph C3.3.4. of this Regulation)

TABLE 4 (continued)

A	B	C
If the individual is a:	and duties require:	then a DNACI/NACI is required:
Naval Academy Midshipman, Military Academy Cadet, or Air Force Academy Cadet	enrollment	to be initiated 90 days after entry
Reserve Officer Training Corps Cadet or Midshipman	entry to advanced course or College Scholarship Program	then a DNACI is required to be initiated 90 days after entry

NOTE 1 - First-term enlistees shall require an ENTNAC.

NOTE 2 - Provided DD Form 398-2 is favorably reviewed, local records check favorably accomplished, and DNACI initiated.

NOTE 3 - Provided an authority designated in Appendix 5 finds delay in such appointment would be harmful to national security; favorable review of DD Form 398-2; NACI initiated; favorable local records check accomplished.

TABLE 5
GUIDE FOR REQUESTING NATIONAL AGENCY CHECKS (NAC)

A	B	C
If the individual is a:	and duties require:	then a NAC is required:
a first-term enlistee	retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT three (3) work days after entry (note 1)
prior service member reentering military service after break in Federal employment exceeding 1 year	Retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT three (3) work days after reentry
nominee for military education and orientation program	education and orientation of military personnel	before performing duties (note 2)
U.S. national military, DoD civilian, or contractor employee	access to restricted areas, sensitive information, or equipment as defined in paragraph C3.6.2.	before authorizing entry
nonappropriated fund instrumentality (NAFI) civilian employee (reference (u))	appointment as NAFI custodian	before appointment
	accountability for nonappropriated funds	before completion of probationary period
	fiscal responsibility as determined by NAFI custodian	before completion of probationary period
	other "positions of trust"	before appointment
Persons requiring access to chemical agents chemical agents	access to or security of chemical agents	before appointment

NOTE: 1 - Request ENTNAC only.

NOTE: 2 - Except where personnel whose country of origin is a country listed at Appendix 7, a BI will be required (See paragraph C3.6.12.).

TABLE 5 (continued)

A	B	C
If the individual is a:	and duties require:	then a NAC is required:
U.S. national, civilian employee nominee for customs inspection duties	waiver under provisions of paragraph C3.6.4.	before appointment (note 3)
Red Cross/United Services Organization personnel	assignment with the Armed Forces overseas	before assignment (see note 4 for foreign national personnel)
U.S. national	DoD building pass	prior to issuance
Foreign national employed overseas	no access to classified information	prior to employment (note 4)

NOTE: 3 - A NAC not over 5 years old suffices unless there has been a break in employment over 12 months. Then a current NAC is required.

NOTE: 4 - In such cases, the NAC shall consist of: (a) Host government law enforcement and security agency record checks at the city, state (province), and national level, and (b) DCII.

AP4. APPENDIX 4

REPORTING OF NONDEROGATORY CASES

AP4.1.1. Background Investigation (BI) and Special Background Investigation (SBI) shall be considered as devoid of significant adverse information unless they contain information listed below:

AP4.1.1.1. Incidents, infractions, offenses, charges, citations, arrests, suspicion or allegations of illegal use or abuse of drugs or alcohol, theft or dishonesty, unreliability, irresponsibility, immaturity, instability or recklessness, the use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

AP4.1.1.2. All indications of moral turpitude, heterosexual promiscuity, aberrant, deviant, or bizarre sexual conduct or behavior, transvestitism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, wife-swapping, window-peeping, and similar situations from whatever source. Unlisted full-time employment or education; full-time education or employment that cannot be verified by any reference or record source or that contains indications of falsified education or employment experience. Records or testimony of employment, education, or military service where the individual was involved in serious offenses or incidents that would reflect adversely on the honesty, reliability, trustworthiness, or stability of the individual.

AP4.1.1.3. Foreign travel, education, visits, correspondence, relatives, or contact with persons from or living in a foreign country of foreign intelligence service.

AP4.1.1.4. Mental, nervous, emotional, psychological, psychiatric, or character disorders/behavior or treatment reported or alleged from any source.

AP4.1.1.5. Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy, or evidence of living beyond the individual's means.

AP4.1.1.6. Any other significant information relating to the criteria included in C2.2.1.1. through C2.2.1.17. or Appendix 8 of this Regulation.

AP5. APPENDIX 5

DoD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES

AP5.1. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE PERSONNEL SECURITY CLEARANCES (TOP SECRET, SECRET, AND CONFIDENTIAL)

AP5.1.1. Secretary of Defense and/or single designee.

AP5.1.2. Secretary of the Army and/or single designee. [1]

AP5.1.3. Secretary of the Navy and/or single designee. [1]

AP5.1.4. Secretary of the Air Force and/or single designee. [1]

AP5.1.5. Chairman of the Joint Chiefs of Staff and/or single designee.

AP5.1.6. Director, Washington Headquarters Services, and/or single designee.

AP5.1.7. Director, National Security Agency, and/or single designee. [1, 2]

AP5.1.8. Director, Defense Intelligence Agency, and/or single designee. [1]

AP5.1.9. Deputy General Counsel, Legal Counsel, OGC, and/or single designee (for contractors under the Defense Industrial Security Program (DISP))

AP5.1.10. Director, Defense Investigative Service, and/or single designee, (may grant security clearances only for contractor personnel under the DISP)

---

[1] Authority to grant, deny or revoke access to SCI is a function of the Senior Officials of the Intelligence Community (SOIC), or their designated representative, as identified in E.O. 12333 (reference (h)) and Director of Central Intelligence Directive (DCID) 1/14 (reference (l)). The authority for making SCI access determinations may also be the same official making security clearance determinations.

[2] Reference to the Director, NSA or single designee is not intended to infringe upon the authorities or responsibilities contained in DoD Directive 5210.45, "Personnel Security in the National Security Agency," reference (i).

AP5.2. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE LAA

Officials listed in subsection AP5.1.1. through AP5.1.10., above, and the Commanders of the Combatant Commands, or their single designee, (must be at general officer, flag rank or civilian equivalent).

AP5.3. OFFICIALS AUTHORIZED TO CERTIFY PERSONNEL UNDER THEIR JURISDICTION FOR ACCESS TO CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

See enclosure to DoD Directive 5210.2 (reference (z)).

AP5.4. OFFICIAL AUTHORIZED TO APPROVE PERSONNEL FOR ASSIGNMENT TO PRESIDENTIAL SUPPORT ACTIVITIES

The Executive Secretary to the Secretary of Defense and the Deputy Secretary of Defense, or designee.

AP5.5. OFFICIALS AUTHORIZED TO GRANT ACCESS TO SIOP-ESI

AP5.5.1. Director of Strategic Target Planning

AP5.5.2. Director, Joint Staff.

AP5.5.3. Chief of Staff, U.S. Army.

AP5.5.4. Chief of Naval Operations.

AP5.5.5. Chief of Staff, U.S. Air Force.

AP5.5.6. Commandant of the Marine Corps.

AP5.5.7. Commanders of the Combatant Commands.

AP5.5.8. The authority may be further delegated in writing by the officials in subsections AP5.5.1. through AP5.5.7. to the applicable subordinates.

AP5.6. FINAL DETERMINATIONS

Three member PSAB shall be formed under the auspices of the following officials to render final determinations when an unfavorable personnel security determination is appealed under paragraph C8.2.2.4. of this Regulation.

AP5.6.1. Secretary of the Army.

AP5.6.2. Secretary of the Air Force.

AP5.6.3. Secretary of the Navy.

AP5.6.4. Chairman of the Joint Chiefs of Staff.

AP5.6.5. Director, NSA.

AP5.6.6. Director, DIA.

AP5.6.7. Director, WHS.

AP5.6.8. General Counsel, Department of Defense (contractors only).

AP5.7. OFFICIALS AUTHORIZED TO SUSPEND ACCESS TO CLASSIFIED INFORMATION

AP5.7.1. Security Clearances

AP5.7.1.1. Contractor Personnel. The Director, Counterintelligence and Security Programs; ODASD(I&S); OASD(C3I); and the Deputy General Counsel (Legal Counsel), Office of General Counsel, OSD.

AP5.7.1.2. Military and/or Civilian Personnel. Commander and/or Agency head, Head of the Component, or adjudicative authority.

AP5.7.2. SCI. Cognizant SOICs, or their designees.

AP5.8. OFFICIALS AUTHORIZED TO ISSUE INTERIM CLEARANCES

AP5.8.1. Interim TOP SECRET clearances may be issued by the officials listed in section AP5.1., above. That may be further delegated on determination by the Head of the Agency.

AP5.8.2. Interim SECRET and/or CONFIDENTIAL clearances may be issued by the officials listed in section AP5.1., above, as well as by organizational commanders.

AP5.9. OFFICIALS AUTHORIZED TO DESIGNATE NONAPPROPRIATED FUND POSITIONS OF TRUST

The Heads of the DoD Components, or their designees.

AP6. APPENDIX 6

GUIDELINES FOR CONDUCTING PRE-NOMINATION PERSONAL INTERVIEWS

AP6.1. PURPOSE

The purpose of the personal interview is to assist in determining the acceptability of an individual for nomination and further processing for a position requiring an SBI.

AP6.2. SCOPE

Questions asked during the course of a personal interview must have a relevance to a security determination. Care must be taken not to inject improper matters into the personal interview. For example, religious beliefs and affiliations, beliefs and opinions regarding racial matters, political beliefs and affiliations of a nonsubversive nature, opinions regarding the constitutionality of legislative policies, and affiliations with labor unions and fraternal organizations are not proper subjects for inquiry. Department of Defense representatives conducting personal interviews should always be prepared to explain the relevance of their inquiries. Adverse inferences shall not be drawn from the refusal of a person to answer questions the relevance of which has not been established.

AP6.3. THE INTERVIEWER

Except as prescribed in section AP6.2., above, persons conducting personal interviews normally will have broad latitude in performing this essential and important function and, therefore, a high premium must necessarily be placed upon the exercise of good judgment and common sense. To insure that personal interviews are conducted in a manner that does not violate lawful civil and private rights or discourage lawful political activity in any of its forms, or intimidate free expression, it is necessary that interviewers have a keen and well-developed awareness of and respect for the rights of interviewees. Interviewers shall never offer an opinion as to the relevance or significance of information provided by the interviewee to eligibility for access to SCI. If explanation in this regard is required, the interviewer will indicate that the sole function of the interview is to obtain information and that the determination of relevance or significance to the individual's eligibility will be made by other designated officials.

AP6.4. INTERVIEW PROCEDURES

AP6.4.1. The Head of the DoD Component concerned shall establish uniform procedures for conducting the interview that are designed to elicit information relevant to making a determination of whether the interviewee, on the basis of the interview and other locally available information (DD 398, "Personnel Security Investigation Questionnaire," personnel records, security file, etc.), is considered acceptable for nomination and further processing.

AP6.4.2. Such procedures shall be structured to insure the interviewee his full rights under the Constitution of the United States, the Privacy Act of 1974 (reference (m)), and other applicable statutes and regulations.

AP6.5. PROTECTION OF INTERVIEW RESULTS

All information developed during the course of the interview shall be maintained in personnel security channels and made available only to those authorities who have a need-to-know in connection with the processing of an individual's nomination for duties requiring access to SCI or those who need access to information either to conduct the required SBI or to adjudicate the matter of the interviewee's eligibility for access to SCI, or as otherwise authorized by Executive order or statute.

AP6.6. ACCEPTABILITY DETERMINATION

AP6.6.1. The determination of the interviewee's acceptability for nomination for duties requiring access to sensitive information shall be made by the commander, or designee, of the DoD organization that is considering nominating the interviewee for such duties.

AP6.6.2. Criteria guidelines contained in DCID 1/14 (reference (l)), upon which the acceptability for nomination determination is to be based shall be provided to commanders of DoD organizations who may nominate individuals for access to SCI and shall be consistent with those established by the Senior Officer of the Intelligence Community of the Component concerned with respect to acceptability for nomination to duties requiring access to SCI.

AP7. APPENDIX 7

(RESERVED FOR FUTURE USE)

AP8. APPENDIX 8

ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMAITON

PURPOSE

The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by Government Departments and Agencies in all final clearance determinations.

ADJUDICATIVE PROCESS

The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- The nature, extent, and seriousness of the conduct.
- The circumstances surrounding the conduct, to include knowledgeable participation.
- The frequency and recency of the conduct.
- The individual's age and maturity at the time of the conduct.
- The voluntariness of participation.
- The presence or absence of rehabilitation and other pertinent behavioral changes.
- The motivation for the conduct.
- The potential for pressure, coercion, exploitation, or duress.
- The likelihood of continuation or recurrence.

Each case must be judged on its own merits and final determination remains the responsibility of the specific Department or Agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security and considered final.

The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following:

A. Allegiance to the United States
B. Foreign influence
C. Foreign preference
D. Sexual behavior
E. Personal conduct
F. Financial considerations
G. Alcohol consumption
H. Drug involvement
I. Emotional, mental, and personality disorders
J. Criminal conduct
K. Security violations
L. Outside activities
M. Misuse of Information Technology Systems

Each of the foregoing should be evaluated in the context of the whole person.

Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior.

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

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

(1) voluntarily reported the information;
(2) sought assistance and followed professional guidance, where appropriate;
(3) resolved or appears likely to favorably resolve the security concern;
(4) has demonstrated positive changes in behavior and employment;
(5) should have his or her access temporarily suspended pending final adjudication of the information.

If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

The information in bold print at the beginning of each adjudicative guideline provides a brief explanation of its relevance in determining whether it is clearly consistent with the interest of national security to grant or continue a persons eligibility for access to classified information.

ADJUDICATIVE GUIDELINES

ALLEGIENCE TO THE UNITED STATES

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

Conditions that could raise a security concern and may be disqualifying include:

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

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

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

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

Conditions that could mitigate security concerns include:

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

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

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

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

FOREIGN INFLUENCE

A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are: (1) not citizens of the United States or (2) may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Conditions that could raise a security concern and may be disqualifying include:

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

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

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

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

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

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

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

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

Conditions that could mitigate 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;

(2) contacts with foreign citizens are the result of official U.S. Government business;

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

(4) the individual has promptly reported to proper authorities all contacts, requests, or threats from persons or organizations from a foreign country, as required;

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

FOREIGN PREFERENCE

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

Conditions that could raise a security concern and may be disqualifying include:

(1) the exercise of dual citizenship;
(2) possession and/or use of a foreign passport;
(3) military service or a willingness to bear arms for a foreign country;
(4) accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;
(5) residence in a foreign country to meet citizenship requirements;
(6) using foreign citizenship to protect financial or business interests in another country;
(7) seeking or holding political office in the foreign country;
(8) voting in foreign elections; and
(9) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

(1) dual citizenship is based solely on parents' citizenship or birth in a foreign country;
(2) indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;
(3) activity is sanctioned by the United States;
(4) individual has expressed a willingness to renounce dual citizenship.

SEXUAL BEHAVIOR

Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, subjects the individual to undue influence or coercion, or reflects lack of judgment or discretion.[1] (Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.)

Conditions that could raise a security concern and may be disqualifying include:

(1) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
(2) compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;
(3) sexual behavior that causes an individual to be vulnerable to undue influence or coercion;
(4) sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

Conditions that could mitigate security concerns include:

(1) the behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;
(2) the behavior was not recent and there is no evidence of subsequent conduct of a similar nature;
(3) there is no other evidence of questionable judgment, irresponsibility, or emotional instability;
(4) the behavior no longer serves as a basis for undue influence or coercion.

---

[1] The adjudicator should also consider guidelines pertaining to criminal conduct (criterion J); or emotional, mental, and personality disorders (criterion I), in determining how to resolve the security concerns raised by sexual behavior.

PERSONAL CONDUCT

Conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

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

(2) refusal to complete required security forms, releases, or provide full, frank and true answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and may be disqualifying also include:

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

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

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

(4) personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or pressure;

(5) a pattern of dishonesty or rule violations[2];

(6) association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

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

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

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

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

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

(6) a refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

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

---

[2] To include violation of any written or recorded agreement made between the individual and the Agency.

FINANCIAL CONSIDERATIONS

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

Conditions that could raise a security concern and may be disqualifying include:

(1) a history of not meeting financial obligations;
(2) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filling deceptive loan statements, and other intentional financial breaches of trust;
(3) inability or unwillingness to satisfy debts;
(4) unexplained affluence;
(5) financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include:

(1) the behavior was not recent;
(2) it was an isolated incident;
(3) the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);
(4) the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
(5) the affluence resulted from a legal source; and
(6) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

ALCOHOL CONSUMPTION

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

Conditions that could raise a security concern and may be disqualifying include:

(1) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other incidents related to alcohol use;
(2) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;
(3) diagnosis by a credentialed medical professional[3] of alcohol abuse or alcohol dependence;
(4) habitual or binge consumption of alcohol to the point of impaired judgment;
(5) consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional[3] and following completion of an alcohol rehabilitation program

Conditions that could mitigate security concerns include:

(1) the alcohol related incidents do not indicate a pattern;
(2) the problem occurred a number of years ago and there is no indication of a recent problem;
(3) positive changes in behavior supportive of sobriety;
(4) following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional.[3]

---

[3] credentialed medical professional: licensed physician, licensed clinical psychologist, or board-certified psychiatrist.

DRUG INVOLVEMENT

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

Drugs are defined as mood and behavior altering:

(a) drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens) and

(b) inhalants and other similar substances.

Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and may be disqualifying include:

(1) any drug abuse (see above definition);

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

(3) failure to successfully complete a drug treatment program prescribed by a credentialed medical professional.[3] Current drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination

Conditions that could mitigate security concerns include:

(1) the drug involvement was not recent;
(2) the drug involvement was an isolated or infrequent event;
(3) a demonstrated intent not to abuse any drugs in the future;
(4) satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.[3]

---

[3] credentialed medical professional: licensed physician, licensed clinical psychologist, or board-certified psychiatrist.

EMOTIONAL, MENTAL, AND PERSONALITY DISORDERS

Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability.

When appropriate, a credentialed mental health professional,[4] acceptable to or approved by the Government, should be consulted so that potentially disqualifying and mitigating information may be fully and properly evaluated.

Conditions that could raise a security concern and may be disqualifying include:

(1) a diagnosis by a credentialed mental health professional [4] that the individual has a disorder that could result in a defect in psychological, social, or occupational functioning;

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

(3) a pattern of high-risk, irresponsible, aggressive, anti-social, or emotionally unstable behavior;

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

Conditions that could mitigate security concerns include:

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

(2) recent diagnosis by a credentialed mental health professional[4] that an individual's previous emotional, mental, or personality disorder is cured or in remission and has a low probability of recurrence or exacerbation;

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

---

[4] credentialed mental health professional: licensed clinical psychologist, licensed social worker, or board-certified psychiatrist.

CRIMINAL CONDUCT

A history or pattern of criminal activity creates doubt about a persons judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

(1) any conduct, regardless of whether the person was formally charged;
(2) a single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

(1) the behavior was not recent;
(2) the crime was an isolated incident;
(3) the person was pressured or coerced into committing the act and those pressures are no longer present in that persons life;
(4) the person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;
(5) there is clear evidence of successful rehabilitation.

SECURITY VIOLATIONS

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

Conditions that could raise a security concern and may be disqualifying include:

(1) unauthorized disclosure of classified information;
(2) violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

(1) were inadvertent;
(2) were isolated or infrequent;
(3) were due to improper or inadequate training;
(4) demonstrate a positive attitude towards the discharge of security responsibilities.

OUTSIDE ACTITIVITIES

Involvement in certain types of outside employment or activities is of security concern if it poses conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and may be disqualifying include:

Any service, whether compensated, volunteer, or employment with:

(1) a foreign country;
(2) any foreign national;
(3) a representative of any foreign interest;
(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Conditions that could mitigate security concerns include:

(1) evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;
(2) the individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

Information Technology Systems include all related equipment used for the communication, mission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

(1) Illegal or unauthorized entry into any information technology system;
(2) Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;
(3) Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
(4) Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

Conditions that could mitigate security concerns include:

(1) The misuse was not recent or significant;
(2) The conduct was unintentional or inadvertent;
(3) The introduction or removal of media was authorized;
(4) The misuse was an isolated event;
(5) The misuse was followed immediately by a prompt, good faith effort to correct the situation.

AP9. APPENDIX 9

OVERSEAS INVESTIGATIONS

AP9.1. PURPOSE

The purpose of this appendix is to establish, within the framework of this Regulation, DoD Directive 5105.42, and Defense Investigative Service Manual 20-1-M (references (hh) and (ii)), standardized procedures for the military investigative agencies to follow when they perform administrative and investigative functions on behalf of DIS at overseas locations.

AP9.2. TYPE INVESTIGATION

This Regulation describes in detail Background Investigations (BI) which are conducted for Limited Access Authorizations (LAA) and those Special Investigative Inquiries (SII) conducted for post-adjudicative purposes. Hereafter they are referred to as LAA and post-adjudicative cases and are briefly described in paragraphs AP9.2.1. and AP9.2.2., below:

AP9.2.1. Limited Access Authorization (LAA). A level of access to classified defense information that may be granted to a non-US citizen under certain conditions, one of which is that a BI must have been completed with satisfactory results. Paragraph C3.4.4. further describes LAA cases.

AP9.2.2. Post-Adjudication Investigation. A Personnel Security Investigation (PSI) predicated on new, adverse or questionable security, suitability or hostage information that arises and requires the application of investigation procedures subsequent to adjudicative action on a DoD-affiliated person's eligibility for continued access to classified information, assignment to or retention in sensitive duties or other designated duties requiring such investigation. While these cases are normally predicated on the surfacing of unfavorable information subsequent to favorable adjudication, they may also be opened when favorable information is offered to counter a previous unfavorable adjudication. Paragraph C2.4.3.3. further describes these cases.

AP9.3. GENERAL

AP9.3.1. As a rule, investigative activity in most PSIs occurs in the United States even when the Subject is at an overseas location. Therefore, the submission of requests for investigation to the Personnel Investigation Center (PIC) at Baltimore is a required procedure as it ensures uniform application of DoD PSI policy and the efficient dispatch and coordination of leads.

AP9.3.2. When the purpose of the investigation is for an LAA or post-adjudication on a Subject overseas, much, if not all of the leads are at an overseas location. While these cases also may be submitted directly to PIC for action, there is an inherent delay in the mailing of the request, the exchange of leads and reports with PIC, and transmittal of the reports back to the requestor. To avoid this delay, the military investigative agencies, when acting for DIS overseas in accordance with DoD Directive 5105.42 (reference (hh) may, with their Headquarters approval, accept these requests for investigations, initiate them and disseminate the results from the same level as they open, close, and disseminate their own cases. Usually this will greatly improve response time to the requester.

AP9.3.3. Under the procedures in paragraph AP9.3.2., above, DIS will not often be in a position to directly exercise its responsibility for control and direction until the case or lead is in progress or even completed; therefore, adherence to the policy stated in referenced documents, and as modified herein, is mandatory. When the policy of the military investigative agency is at variance with the above, the matter will be referred to the respective headquarters for resolution.

AP9.3.4. Since DIS is ultimately responsible for the personnel security product, it must be kept informed of all such matters referred to in this appendix. For instance, when the investigative agency overseas receives a DD Form 1879, "Request for Personnel Security Investigation," which sets forth an issue outside DIS jurisdiction, it will reject the request, inform the requester of the reason and furnish an information copy of the DD Form 1879 and rejection letter to PIC. When the issue/jurisdiction is unclear to the investigative agency, the DD Form 1879 and the perceived jurisdictional question should be promptly forwarded to DIS for action and, if appropriate, to the Component' s headquarters for information. Questions on the interpretation of DIS or DoD policy and Directives pertaining to individual PSI cases can usually be resolved through direct communications with PIC.

AP9.3.5. DoD Directive 5105.42 (reference (hh)), establishes the supporting relationship of the military investigative agencies to DIS in overseas areas, and DIS provides these Agencies with copies of relevant policy and interpretive guidance. For

these reasons, the investigative agency vice the requester, is responsible for evaluating the request, processing it, collecting and evaluating the results within their jurisdiction for sufficiency, and forwarding the completed product to the appropriate activity.

AP9.3.6. The magnitude of operations at PIC requires that methods of handling LAA and post-adjudicative cases be consistent to the maximum extent possible. For this reason, the procedures for LAA cases are nearly identical to those for post-adjudicative cases. Briefly, the main exceptions are:

AP9.3.6.1. The notification to PIC that a post-adjudication case has been opened will be by message, since an issue is present at the outset, whereas notification of an LAA case should normally be by mail.

AP9.3.6.2. The scope of the LAA investigation is 10 years or since the person's 18th birthday, whichever is shortest, whereas the leads in a post-adjudication case are limited to resolving the issue.

AP9.4. JURISDICTION

AP9.4.1. As set-forth in DoD Directive 5105.42 (reference (hh), DIS is responsible for conducting all DoD PSIs in the 50 States, District of Columbia, and Puerto Rico, and will request the Military Departments to accomplish investigative requirements elsewhere. The military investigative agencies in overseas locations routinely respond to personnel security investigative leads for DIS.

AP9.4.2. DIS jurisdiction also includes investigation of subversive affiliations, suitability information, and hostage situations when such inquiries are required for personnel security purposes; however, jurisdiction will rest with the military investigative agencies, FBI and/or civil authorities as appropriate when the alleged subversion or suitability issue represents a violation of law or, in the case of a hostage situation, there is an indication that the person concerned is actually being pressured, coerced, or influenced by interests inimical to the United States, or that hostile intelligence is taking action specifically directed against that person. Specific policy guidance on the applicability of these procedures and the jurisdictional considerations are stated in C2.4.

AP9.5. CASE OPENING

AP9.5.1. A request for investigation must be submitted by using DD Form 1879 and accompanied by supporting documentation unless such documentation is not immediately available, or the obtaining of documentation would compromise a sensitive investigation. Upon receipt of the request, the military investigative component will identify the issue(s), scope the leads, and ensure that the proposed action is that which is authorized for DIS as delineated in this Regulation, DoD Directive 5105.42 and Defense Investigative Service 20-1-M (references (hh) and (ii)).

AP9.5.2. Upon such determination, the Component will prepare an Action Lead Sheet (ALS), which fully identifies the Subject and the scope of the case, and specifies precisely the leads that each investigative Component (including DIS/PIC when appropriate) is to conduct.

AP9.5.3. Case opening procedures described above are identical for LAA and post-adjudication cases except with respect to notification of case opening to PIC:

AP9.5.3.1. Post-Adjudication Cases. These cases, because they involve an issue, are potentially sensitive and must be examined as early as possible by PIC for conformity to the latest DoD policy. Accordingly, the initial notification to PIC of case openings will always be by message. The message will contain at a minimum:

AP9.5.3.1.1. Full identification of the subject;

AP9.5.3.1.2. A narrative describing the allegation/facts in sufficient detail to support opening of the case; and

AP9.5.3.1.3. A brief listing of the leads that are planned. The DD Form 1879 and supporting documents, along with the Agency's ALS, should be subsequently mailed to PIC.

AP9.5.3.2. LAA Cases. The notification to PIC of case opening will normally be accomplished by mailing the DD Form 1879, DD Form 398, "Personal History Statement," a copy of the ALS, and any other supporting documents to PIC. Message notification to PIC in LAA cases will only be required if there is a security or suitability issue apparent in the DD Form 1879 or supporting documents.

AP9.5.4. Beyond initial actions necessary to test allegation for investigative merit and jurisdiction, no further investigative action should commence until the notification of case opening to PIC has been dispatched.

AP9.5.5. PIC will promptly respond to the notification of case opening by mail or message specifying any qualifying remarks along with a summary of previously existing data. PIC will also provide a DIS case control number (CCN). This number must be used by all Components on all case-related paperwork/reports.

(The investigating agency may assign its unique Service CCN for interim internal control; however, the case will be processed, referenced, and entered into the DCII by the DIS case control number.) The first five digits of the DIS CCN will be the Julian date of the case opening when received at DIS.

AP9.6. CASE PROCESSING

AP9.6.1. The expected completion time for leads in LAA cases is 50 calendar days and for post-adjudication cases, 30 days, as computed from the date of receipt of the request. If conditions preclude completion in this time period, a pending report of the results to date, along with an estimated date of completion will be submitted to PIC.

AP9.6.2. Copies of all ALSs will be furnished to PIC. In addition, PIC will be promptly notified of any significant change in the scope of the case, or the development of an investigative issue.

AP9.6.3. The procedures for implementing the Privacy Act in PSI cases are set in DIS 20-1-M (reference (ii)). Any other restrictions on the release of information imposed by an overseas source or by regulations of the country where the inquiry takes place will be clearly stated in the report.

AP9.6.4. The report format for these cases will be that used by the military investigative agency.

AP9.6.5. Investigative action outside the jurisdictional area of an investigative component office may be directed elsewhere by ALS as needed in accordance with that Agency's procedures and within the following geographical considerations:

AP9.6.5.1. Leads will be sent to PIC if the investigative action is in the United States, District of Columbia, Puerto Rico, American Samoa, Bahama Islands, the U.S. Virgin Islands, and the following islands in the Pacific: Wake, Midway, Kwajalin, Johnston, Carolines, Marshalls, and Eniwetok.

AP9.6.5.2. Leads to areas not listed above may be dispatched to other units of the investigative agency or even to another military agency's field units if there is an

agreement or memorandum of understanding that provides for such action. For case accountability purposes, copies of such "lateral" leads must be sent to the PIC.

AP9.6.5.3. Leads that cannot be dispatched as described in subparagraph AP9.6.5.2., above, and those that must be sent to a non-DoD investigative agency should be sent to PIC for disposition.

AP9.6.6. The Defense Investigative Manual (reference (ii)) calls for obtaining PIC approval before conducting a Subject interview on a post-adjudicative investigation. To avoid the delay that compliance with this procedure would create, a military investigative component may conduct the interview provided:

AP9.6.6.1. All other investigative leads have been completed and reviewed.

AP9.6.6.2. The CCN has been received, signifying DIS concurrence with the appropriateness of the investigation.

AP9.6.6.3. Contrary instructions have not been received from the PIC.

AP9.6.6.4. The interview is limited to the resolution of the relevant issues disclosed by the investigation.

AP9.6.7. Notwithstanding the provisions of paragraph AP9.6.1. through AP9.6.4., above, if time is of the essence due to imminent transfer of the subject, a subject interview may be conducted at the discretion of the investigative agency.

AP9.7. CASE RESPONSIBILITY: LAA and PA

Section AP9.3., above, describes the advantages of timely handling that accrue when the military investigative components act for DIS overseas. These actions for DIS may, however, be limited by the Component's staffing and resource limitations, especially since some cases require more administration and management than others. Post-adjudication case leads, for instance, will normally be within the geographical jurisdiction of the Component that accepted the request for investigation; therefore, relatively little case management is required. In contrast, LAA cases may require leads world-wide, and, therefore, create more complex case management and administration, especially in the tracking, monitoring and reviewing of leads outside the Component's geographical area. Accordingly, an investigative Component will accept the case from the requester, but only assign itself the appropriate leads within its own geographical jurisdiction and send the balance to PIC for appropriate disposition in accordance with the following:

AP9.7.1. The investigative agency will accept the request for investigation (thereby saving time otherwise lost in mailing to PIC) but limit its involvement in case management by extracting only those leads it will conduct or manage locally.

AP9.7.2. The Agency should then prepare an ALS that shows clearly what leads it will cover and send PIC a copy of this ALS, along with the request for investigation and any other appropriate documentation. It must be clear in the ALS that PIC is to act on all those leads that the unit has not assigned to itself.

AP9.7.3. PIC, as case manager, will assume responsibility for the complete investigative package and, upon receipt of the last lead, will send the results to the appropriate activity.

AP9.7.4. The Agency that accepted the case and assigned itself leads may send a copy of its report to the activity in the "Results to" block at the same time it sends the originals to PIC. If so, the letter of transmittal must inform the recipient that these reports are only a portion of the investigation, and that the balance will be forthcoming from PIC. Similarly, PIC must be informed of which investigative reports were disseminated. (This is normally done by sending PIC a copy of the letter of transmittal.)

AP9.8. SCOPE

AP9.8.1. LAA. The scope of investigation is 10 years or from age 18, whichever is the shortest period.

AP9.8.2. Post-Adjudication Cases. There is no standard scope. The inquiries conducted will be limited to those necessary to resolve the issue(s).

AP9.9. CASE CLOSING: LAA and PA

AP9.9.1. Whether the investigative Component or PIC closes out an investigation, there are three key elements to consider:

AP9.9.1.1. The investigative results must be reviewed for quality and conformance to policy.

AP9.9.1.2. The results must be sent to the activity listed in the "Results to" block of the DD Form 1879.

AP9.9.1.3. PIC must be informed whether or not any dissemination was made

by the investigative agency and, if so, what reports were furnished.

AP9.9.2. Investigative results may also be sent to a requester or higher level activity that makes a statement of need for the results. In such instances, a copy of the letter requesting the results and the corresponding letter of transmittal must be sent to PIC for retention.

AP9.9.3. When an investigative agency disseminates reports for PIC, it may use the transmittal documents, letters, or cover sheets it customarily uses for its own cases.

AP9.9.4. The material that is to be provided to PIC will consist of: The originals of all reports, and all other case documentation such as original statements, confidential source sheets, interview logs, requests for investigation, letters of transmittal to adjudicaters/requesters, or communications with the requester, such as those that modify the scope of the investigation.

AP9.9.5. For DIS to fulfill its responsibilities under DoD 5220.22-R (reference (a)) and the Privacy Act of 1974 (reference (m)), all inquires conducted in its behalf must be set forth in an ROI for the permanent file, whether the case is completed, terminated early or referred to another Agency.

AP9.10. REFERRAL

A case may require premature closing at any time after receipt of the DD Form 1879 by the investigative Component if the information accompanying the request, or that which is later developed, is outside DIS jurisdiction. For example, alleged violations of law, a counterintelligence matter, or actual coercion/influence in a hostage situation (see paragraph AP9.4.2., above) must be referred to the appropriate Agency, and DIS involvement terminated. The requester will be informed by letter or endorsement to the DD Form 1879 of the information developed that, due to jurisdictional consideration, the case was referred to (fill in appropriate address) and that the DIS case is closed. The Agency to which referral was made and PIC will be furnished with the results of all investigations conducted under DIS auspices. DIS, however, has an interest in the referral Agency's actions and no information should be solicited from that Agency.

AP10. APPENDIX 10

ADP POSITION CATEGORIES AND CRITERIA FOR DESIGNATING POSITIONS

AP10.1. ADP POSITION CATEGORIES AND CRITERIA FOR DESIGNATING POSITIONS

OMB Circular A-71 (and Transmittal Memo #1), July 1978; OMB Circular A-130, December 12, 1985; and FPM Letter 732, November 14, 1978, contain the criteria for designating positions under the existing categories used in the personnel security program for Federal civilian employees as well as the criteria for designating ADP and ADP-related positions. This policy is outlined below:

AP10.2. ADP POSITION CATEGORIES

AP10.2.1. Critical-Sensitive Positions

AP10.2.1.1. ADP-I positions. Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

AP10.2.2. Noncritical-Sensitive Positions

AP10.2.2.1. ADP-II positions. Those positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system.

AP10.2.3. Nonsensitive Positions

AP10.2.3.1. ADP-III positions. All other positions involved in computer activities. In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower categories based on the Agency's judgement as to the unique characteristics of the system or the safeguards protecting the system.

AP10.3. CRITERIA FOR DESIGNATING POSITIONS

Three categories have been established for designating computer and computer-related positions -- ADP-I, ADP-II, and ADP-III. Specific criteria for assigning positions to one of these categories is as follows:

Category	Criteria
ADP-I	Responsibility or the development and administration of Agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.
	Significant involvement in life-critical or mission-critical systems.
	Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
	Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if.the activities of the individual are not subject to technical review by higher authority in the ADP-I category to insure the integrity of the system.
	Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
	Other positions as designated by the Agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.
ADP-II	Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP-I category, includes, but is not limited to:
	(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;
	(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by the Agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP-I positions.
ADP-III	All other positions involved in Federal computer activities.

AP11. APPENDIX 11

LIST OF SAMPLE NOTIFICATIONS

Initial Package to Notify Organization and Individual

Local Organization Letter with SOR	166
Sample SOR (Enclosure 1 to Letter)	168
Security Concerns and Supporting Adverse Information	169
Instructions for Responding to SOR	170
Sample Applicable Personnel Security Guidelines (Enclosure 2 to Letter)	173
SOR Receipt and Statement of Intention (Enclosure 3 to Letter)	174

Package to Inform Organization and Individual of Denial

Local Organization Letter with LOD	176
Sample Letter of Denial (Enclosure to Letter)	178
Notice of Intent to Appeal	180
Instructions for Appealing a Letter of Denial/Revocation (LOD)	181

Local Organization Letter with Statement of Reasons (SOR)

From: Director, (Component) Central Adjudication Facility
To: Director, Service Graphics Facility, Washington, DC

Subject: RESPONSIBILITY FOR HANDLING STATEMENT OF REASONS (SOR)

Reference: (a) (Component Personnel Security Regulation)

Enclosure:
1. SOR
2. SOR Receipt and Statement of Intention
3. Form for Requesting (Personnel Security Investigation)

1. The purpose of this letter is to provide instructions for actions required by your organization related to the individual named in the enclosed SOR. Since denial or revocation of access eligibility can have a severe impact on individuals and their careers, procedures required by reference (a) must be closely followed to ensure that both security and fairness requirements are met.

2. Your organization is responsible for completing the following actions with regard to the individual named in the SOR:

a. Consider whether or not to suspend access to classified information and assignment of the individual to nonsensitive duties pending a final personnel security decision. Failure to do so could result in an increased level of security risk.

b. Designate a person from your organization as the point of contact (POC) in this matter pursuant to paragraph 8-201(a), reference (a), above. This person will serve as a liaison between the (Component) Central Adjudication Facility (CAF) and the individual.

3. The POC from your organization should:

a. Promptly deliver enclosure (1) to this letter, the SOR and its enclosures, to the named individual.

b. Complete and forward enclosure (2) to this letter to the CAF within 10 calendar days. Ensure that Parts I, II, and III are all completed. This form notifies the CAF whether the individual intends to respond to the SOR and whether your organization has granted a time extension.

c. Advise the individual that he or she should not attempt to communicate directly with the CAF except in writing, and that, if necessary, he or she should seek the assistance of your organization's designated POC. Also, ensure that the individual understands that he or she is entitled to obtain legal counsel or other assistance but that this must be done at the individual's own expense.

d. Ensure that the individual understands the consequences of being found ineligible for access to classified information and performance of sensitive duties and the serious effect such a determination could have on his or her career.

e. Take particular care to ensure that the individual fully understands that the proposed denial or revocation action will become final if your organization notifies the CAF via enclosure (2) that the individual does not intend to respond to the SOR. Ensure that the individual understands that failure to submit a timely reply will result in forfeiture of any further opportunity to contest this unfavorable personnel security determination.

f. Explain procedures for requesting a time extension for responding to the SOR. If the individual requires additional time to obtain copies of investigative records and/or to prepare his or her response, your organization may grant an extension of up to 30 additional calendar days. The CAF must be notified of such an extension using enclosure (2). See reference (a) for more detail.

g. Assist the individual in obtaining applicable references and copies of pertinent investigative files. The SOR is usually based on investigative information from the Defense Investigative Service (DIS) and/or another investigative agency. If the individual desires copies of releasable information pertinent to this SOR, a request may be submitted to the CAF using the receipt at enclosure (2). If the individual wants to obtain a copy of the complete investigative file, provide him or her with enclosure (3) which is the form for requesting [DIS and/or other investigative agency] records under the Privacy Act (5 U.S.C. 552a.).

4. Ensure that the individual's response to the SOR is promptly endorsed by appropriate authority and immediately forwarded to the CAF. Submissions to the CAF are deemed to have been made when actually received by the CAF, or postmarked, whichever is sooner. This endorsement should include observations and comments regarding the person's judgment, reliability and trustworthiness as well as a recommendation regarding the decision at hand. An endorsement that does not include comments and a recommendation will be taken to mean that your organization concurs with the unfavorable personnel security determination.

5. (Additional component-specific requirements)

6. If you have any questions, the point of contact at the CAF is Mr. John Doe, DSN 000-0000 or commercial (000) 000-0000, e-mail doejohn@caf.dod.

Statement of Reasons (SOR)

From: Director, [Component] Central Adjudication Facility
Through: Director, Service Graphics Facility, Washington, DC
To: Mr. John Doe, SSN 000-00-0000

Subject: INTENT TO (DENY/REVOKE) ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT IN SENSITIVE DUTIES

Reference: (a) Component Personnel Security Regulation

Enclosure:
1. Security Concerns and Supporting Adverse Information
2. Instructions for Responding to a Statement of Reasons
3. Applicable Personnel Security Guidelines

1. A preliminary decision has been made to (deny/revoke) your eligibility for access to classified information or employment in sensitive duties. Adverse information from an investigation of your personal history has led to the security concerns listed in enclosure (1) and has raised questions about your trustworthiness, reliability, and judgment. If this preliminary decision becomes final, you will not be eligible for access to classified information or employment in sensitive duties as defined by reference (a).

2. You may challenge this preliminary decision by responding, in writing, with any information or explanation which you think should be considered in reaching a final decision. Enclosure (2) is provided to assist you if you choose to respond. Enclosure (3) provides an extract from reference (a) of the specific personnel security guidelines used in the preliminary decision to (deny/revoke) your eligibility for access to classified information employment in sensitive duties. The preliminary decision will become final if you fail to respond to this letter. You may obtain legal counsel or other assistance; however, you must do so at your own expense.

3. You must notify your (Component) Central Adjudication Facility (CAF) via the head of your organization within 10 calendar days as to whether or not you intend to respond. If you choose not to respond, you will forfeit an opportunity to contest this unfavorable personnel security determination. Should you choose to respond, your response must be submitted via the head of your organization within 30 calendar days from the date you received this letter. Your organization may grant up to 30 additional calendar days if you submit a written request to your security office. Additional time extensions may only be granted by the CAF. Contact the point of contact with the CAF for help in preparing and forwarding your notice of an intent to respond and your response and if you wish to obtain releasable investigative records used in your case.

4. If you currently have access to classified information, this access (is/may be) suspended pending the final decision. Please direct questions regarding this letter to your security officer or the point of contact with the CAF.

Security Concerns and Supporting Adverse Information

Subject of Investigation: (Mr. John Doe, 000-00-0000)

Statement of Reasons

1. Available information tends to show criminal or dishonest conduct on your part:

   a. You were arrested on 28 March 1985 in Arlington, VA, for assault on a police officer. You were found guilty and fined $4,000.

   b. You were arrested on 10 January 1993 in Fairfax, VA, and charged with interfering with an arrest. You were released on $300 bail which you forfeited for failure to appear.

   c. You were arrested on 22 June 1994 in Fairfax, VA, on a bench warrant and charged with failure to appear (as set forth above). You were found guilty of interfering with an arrest on 10 January 1993 (as set forth above) and fined $400. The charge of failure to appear was dismissed.

2. Available information tends to show financial irresponsibility on your part:

   a. You filed for Bankruptcy under Chapter 7 in the U.S. District Court, Washington, DC on 10 August 1987. You were discharged from debts

   b. A judgment was entered against you for $2,500 on 20 July 1992, in the Superior Court, Washington, DC. As of 30 January 1995, the judgment had not been paid.

   c. As of 20 July 1994, your credit account with the Hecht Company, Washington, DC was $350 overdue and referred for collection.

   d. As of 20 July 1994, your credit account with J.C. Penney Co., Arlington, VA, was $500 overdue and referred for collection.

Instructions for Responding to a Statement of Reasons (SOR)

A preliminary decision has been made to deny or revoke your eligibility for access to classified information or employment in sensitive duties. This preliminary decision will automatically become final if you fail to notify the Central Adjudication Facility (CAF) within 10 days that you intend to respond to the SOR. You will also lose your right to appeal that final decision if you do not submit a timely response. If this decision becomes final, you will not be eligible to handle classified information or perform sensitive duties. This could prevent you from continuing in your present position or pursuing your current career.

The SOR is based on adverse information revealed by an investigation into your personal history. Specific security concerns about your conduct or background, along with supporting adverse information, are listed in enclosure (1) to the Statement of Reasons.

These instructions are intended to help you provide the most accurate and relevant information as to why the preliminary decision should be overturned. However, it is only a guide. You should provide whatever information you think ought to be considered in reaching the final decision.

It is in your best interest to provide the most complete and accurate information possible at this stage in the decision-making process. Therefore, if you decide to challenge the preliminary decision, you must respond to the statement of reasons as completely as possible.

A. Before Responding

(1) Follow the instructions. The SOR and these instructions provide specific requirements and deadlines for compliance. You will forfeit your right to appeal if you fail to follow these instructions. You must notify the CAF via the point of contact (POC) within 10 calendar days as to whether or not you intend to respond. Should you choose to respond, your response must be submitted via the head of your organization within 30 calendar days from the date you received the SOR, unless you requested and were granted an extension of time.

(2) Review adverse information. You should carefully read the security concerns and supporting adverse information (enclosure 1) to the SOR to determine if the findings are accurate and whether there are circumstances that were not included and which might have a favorable bearing in your case. You may obtain relevant investigative or other information pertinent to the adverse information listed in enclosure (1) to the SOR. In addition, you may obtain a complete copy of releasable investigative records concerning your personal history under the provisions of the Privacy Act. Your security officer or point of contact with the CAF can help you obtain copies of these records. If you do submit a request for your investigative records, make sure to ask the POC for a time extension to the deadline for responding to the SOR since it may take up to 30 calendar days to receive these records.

(3) Obtain and organize supporting documents. Gather any documentation that supports your case. Documentation should be organized according to the security concerns presented in enclosure (1). The most useful documents will be those that refute, correct, explain, extenuate,

mitigate, or update the adverse information presented in enclosure (1). Examples of useful documentation include copies of correspondence; court records with details or dispositions of arrests and status of probation; receipts; copies of canceled checks or letter from creditors verifying the status of delinquent accounts; certificates of completion for rehabilitation programs; releases from judgment or attachment; transcripts of court testimony taken under oath; probation reports; copies of negotiated plea bargains; etc. Mere statements, such as "I paid those bills," "I didn't do it," or "It wasn't my fault," will not carry as much weight as supporting documentation. You may provide statements from co-workers, supervisors, your commander, friends, neighbors and others concerning your judgment, reliability and trustworthiness, and any other information that you think ought to be considered before a final decision is made.

(4). Seek assistance. An individual at your organization has been designated as a point of contact with the CAF on this matter. If this person cannot answer your questions, he or she can request assistance from higher authority. The process is designed so that individuals can represent themselves. Nonetheless, you may obtain legal counsel or other assistance in preparing your response. However, if you obtain assistance, it must be at your own expense.

Remember -- it is up to you to decide whether to respond. You are responsible for the substance of your response and it must be signed by you.

B. Writing a Response

(1) Your response should be in the form of a letter from you to the CAF. You should address each security concern separately. You should admit or deny each security concern and admit or deny each item of supporting adverse information.

(2) It is essential that you address each security concern and the adverse information cited to support it. Provide any information that explains, refutes, corrects, extenuates, mitigates or updates each security concern. Include, wherever possible, copies of the types of documents described above. Organize supporting documents in the order that they are referred to in your letter and enclose copies with your letter. Finally, be sure to sign and date your letter.

(3) The impact of your response will depend on the extent to which you can specifically refute, correct, extenuate, mitigate, or update security concerns and adverse information presented in enclosure (1). Information that is untrue should be specifically refuted. If you believe that the adverse information, though true, does not support the security concern or presents an incomplete picture, you should provide information that explains your case. This additional information could help you disprove or lessen the security concern.

(4) Personnel security guidelines are used by decision-makers to determine whether certain adverse information is of security concern. The guidelines pertinent to security concerns in your case are listed in enclosure (3) to the SOR. These guidelines are general rules used by decision-makers in determining whether an individual should be granted eligibility for access to classified information or permitted to perform sensitive duties. The guidelines provide a framework for weighing all available information, both favorable information as well as adverse information

that is of security concern. The guidelines help decision-makers make a common-sense determination concerning an individual's eligibility for access to classified information and performance of sensitive duties based upon all that is known about an individual's personal history.

(5) Place your written response and supporting documents in a single envelope or package and forward it to the CAF via the head of your organization. Your organization will add its comments at that time. An endorsement by your organization that does not include substantive comments and a recommendation will be interpreted to mean that your organization concurs with the SOR. Be sure to meet the time deadlines. You will be notified in writing of the final decision. In most cases this decision will be made within 60 days. If the decision is in your favor, your access eligibility will be granted or restored. If not, you may appeal the decision to a higher authority.

Applicable Personnel Security Guidelines

The relevant personnel security guidelines are listed below for each area of security concern in your case. The security concerns and supporting adverse information are provided in enclosure (1).

Security Concern: Available information tends to show criminal conduct on your part.

A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness. Conditions that signal security concern and may be disqualifying include: (1) any criminal conduct, regardless of whether the person was formally charged; (2) a single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include: (1) the criminal behavior was not recent; (2) the crime was an isolated incident; (3) the person was pressured or coerced into committing the act and those pressures are no longer present in that person's life; (4) the person did not intentionally commit the act and the factors leading to the unintentional violation are not likely to recur; (5) there is clear evidence of successful rehabilitation.

Security Concern: Available information tends to show financial irresponsibility or unexplained affluence on your part.

An individual who is financially overextended is at greater risk of having to choose between significantly reducing lifestyle or engaging in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts. Conditions that signal security concern and may be disqualifying include: (1) a history of not meeting financial obligations resulting in bankruptcy; (2) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust; (3) being unable to satisfy debts incurred to creditors; (4) unexplained affluence; (5) financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include: (1) the behavior was not recent; (2) it was an isolated incident; (3) the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation); (4) the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control; (5) the affluence resulted from a legal source; and (6) the individual initiated a good-faith effort to repay overdue creditors.

SOR Receipt and Statement of Intention

From: Director, Service Graphics Facility
To: Director, (Component) Central Adjudication Facility

Subject: Acknowledgment of Receipt for Statement of Reasons

1. I acknowledge receipt and delivery of your Statement of Reasons (SOR) to Mr. John Doe, SSN 000-00-0000. Parts I, II, III and IV of this form have been completed as requested.

PART I

I have received an SOR on this date from the (Component) Central Adjudication Facility.

_____
(Signature) (Date)

PART II

I intend to:

a. ( ) submit no reply to the SOR.

b. ( ) respond to the SOR but have requested an extensionfor the following reasons:

_____
_____

_____
_____

c. ( ) respond via my organization head within 30 calendar days of the date I acknowledged receipt of the SOR.

_____
_____
(Signature) (Date)

PART III

Check one of the following:

a. ( ) I request relevant copies of documents and records upon which the SOR is based;

b. ( ) I do not desire relevant copies of documents and records upon which the SOR is based.

PART IV

This organization

a. ( ) has not granted an extension.

B. ( ) has granted an extension until

_____ (Date)

Point of Contact:

_____

(Print Name) (Position)

Local Organization Letter with LOD

From: Director, (Component) Central Adjudication Facility
To: Director, Service Graphic Facility, Washington, DC

Subject: RESPONSIBILITIES FOR HANDLING LETTER OF (DENIAL/REVOCATION)

Enclosure: 1. Letter of Denial/Revocation (LOD)
2. LOD Receipt

1. A decision has been made by the Central Adjudication Facility (CAF) to (deny/revoke) the (security clearance, SCI access, employment in sensitive duties) of the individual named in the enclosed LOD. The purpose of this letter is to provide instructions for actions required by your organization.

2. If not already accomplished, your organization is responsible for completing the following actions with regard to the individual named in the LOD:

a. Terminate access to classified information and/or assignment to sensitive duties.

b. Designate a person from your organization as the point of contact in this matter.

3. Your point of contact (POC) on this matter should promptly deliver enclosure (1) to the named individual. Have the individual sign and date enclosure (2) upon receipt of the LOD. This signature verifies receipt of the LOD and should be retained by your organization until the final disposition of the appeal.

4. If the subject responded to the statement of reasons, your POC should:

a. Ensure the individual understands that he has 10 calendar days, from receipt of the LOD, to submit a notice of intent to appeal and to elect whether to appeal in writing to the Personnel Security Appeals Board (PSAB) or to appear in person before a Defense Office of Hearings and Appeals (DOHA) Administrative Judge (AJ). He must notify your organization of his intended action. Any extensions to this deadline must be submitted in writing to the PSAB.

b. Ensure that the individual understands that he may elect to appeal in writing directly to the PSAB or to request a personal appearance before a DOHA AJ. If the individual desires a personal appearance, the request must be in writing. It must be sent to DOHA within 10 calendar days of the individual's receipt of the LOD. If the individual desires to appeal in writing directly to the PSAB, it must be filed within 30 calendar days of receipt of the LOD. A form for the notice of intent to appeal has been provided as an enclosure to the LOD.

5. If the subject did not respond to the statement of reasons, your POC should inform the individual the decision is final and the appeal process is concluded. Exceptions may only be granted by the CAF.

6. If your organization or the named individual has any questions, the POC should communicate with the President, PSAB, at DSN 000-0000 or commercial 000-00-0000, or the Director, DOHA, at Autovon 226-4598 or commercial 703-696-4598.

Letter of Denial/Revocation(LOD)

From: Director (Component)Central Adjudication Facility
Through: Director, Service Graphic Facility, Washington, D.C.
To: Mr. John Doe, SSN 000-00-0000

Subject: FINAL (DENIAL/REVOCATION) OF ELIGIBILITY FOR ACCESS TO CLASSIFIED
INFORMATION OR (EMPLOYMENT IN SENSITIVE DUTIES)

Reference: (a) Our ltr (Ser XXX) of (date)
(b) Personnel Security Regulation
(c) Your ltr of (date)

Enclosure: 1. Notice of Intent to Appeal
2. Instructions for Appealing a Letter of (Denial/Revocation)

1. Reference (a) informed you of our intent to [deny/revoke] your eligibility for access to classified information (or employment in sensitive duties). An enclosure of this reference listed security concerns and supporting adverse information supporting this preliminary decision. The contents of your response have been carefully considered. Our final assessment of the security concerns presented in reference (a) is as follows:

a. Criminal conduct - The information you provided successfully mitigated the security concerns related to your arrest on 28 March 1985. However, you did not sufficiently address or provide any new information to explain or mitigate the other adverse information (items 1b and 1c). Your criminal conduct is still of security concern.

b. Financial irresponsibility - While you provided an explanation for the Superior Court Judgment, you did not sufficiently address or provide any new information to explain the other adverse information (items 2a, 2c and 2d). Your financial irresponsibility is still of security concern.

2. Given the remaining security concerns, effective this date, we have (denied/revoked) your eligibility for access to classified information and for assignment to a sensitive position using the provisions of reference (b).

3. You may appeal this letter of denial (LOD) in one of two ways: (1) by notifying the Personnel Security Appeal Board (PSAB) within 10 calendar days after you receive this LOD of your intent to appeal directly to the PSAB and by providing the PSAB within the next 30 calendar days with any supporting material not already provided as to why the LOD should be overturned; or (2) by requesting a personal appearance before an Administrative Judge to present your case. If you request a personal appearance, it must be sent to the Director, Defense Office of Hearings and

Appeals (DOHA), Post Office Box 3656, Arlington, Virginia, 22203 (FAX No. 703-696-6865) within 10 calendar days of your receipt of the LOD. A form (enclosure 1) for requesting a personal appearance is appended. In either case, inform the head of your employing organization that you are submitting an appeal. Instructions for preparing and executing an appeal are provided at enclosure 2.

4. If you appeal, the case file including all of the information you supplied in accordance with reference (c) will be forwarded to either the PSAB or the DOHA for consideration. If you require an extension to a deadline, you must make your request in writing to the PSAB or the DOHA and notify the head of your organization.

5. Questions regarding this LOD should be directed to POC designated by your organization.

Use The Following If The Individual Did Not Respond To SOR:

1. Reference (a) informed you of our intent to (deny/revoke) your eligibility for access to classified information and for assignment to sensitive duties.

2. Reference (a) further informed you that the unfavorable personnel security decision would become automatically final if you failed to submit a timely response.

3. Because we have received no timely response, your eligibility for access to classified information or performance of sensitive duties is hereby (denied/revoked). This decision is final and is not subject to further appeal.

Notice of Intent to Appeal

PART I

I, (last name), (first name), (middle initial), social security number (000-00-0000), received a Letter of Denial/Revocation from (Name of CAF) dated MMDDYY. I elect (check one of the following):

( ) to appeal directly to PSAB

( ) a personal appearance before a DOHA Administrative Judge

PART II

The following information is provided so that I can be contacted by the PSAB or DOHA:

a. Duty Address:

b. Duty Phone:

c. Home Address:

d. Home Phone:

PART III

This Notice must be sent to the President of the PSAB (address), or the Director, Defense Office of Hearings and Appeals, Post Office Box 3656, Arlington, Virginia 22203 (FAX No. (703)-696-6865) within 10 calendar days from receipt of the Letter of Denial/Revocation (LOD).

_____

Signature Date

Instructions for Appealing a Letter of Denial/Revocation (LOD)

A decision has been made to deny or revoke your eligibility for access to classified information or performance of sensitive duties. This means that your are not eligible to handle classified information or perform sensitive duties. This could prevent you from continuing in your present position or pursuing your current career. The letter of denial or revocation (LOD) explains this decision. It is based on adverse information which raises security concerns about your trustworthiness, reliability or judgment.

A. How to Appeal

The LOD can be appealed in one of two ways:

1. You may request a personal appearance before an administrative judge (AJ) from the Defense Office of Hearings and Appeals (DOHA). This appearance is intended to provide you with an additional opportunity to present a full picture of your situation. You will have an opportunity to orally respond to the security concerns noted in the LOD and submit supporting documentation to the AJ who will make a recommendation to the Personnel Security Appeal Board (PSAB). The PSAB will consider both your written record and the results of the personal appearance in making its final decision.

2. You may, however, prefer to submit a written appeal to the PSAB and forego the personal appearance. If you submit a written appeal, you may also provide supporting documentation. Having or not having a personal appearance will not bias the PSAB in making a fair determination in your case.

You must elect either (1) or (2); you may not do both.

B. Appealing Without a Personal Appearance

If you choose to appeal without a personal appearance, your written response should provide whatever information you think ought to be considered in the final decision. You should try to specifically explain, refute, extenuate, mitigate or update the security concerns presented in the LOD.

You should review enclosure (2) to the SOR, "Instructions for Responding to a Statement of Reasons (SOR)" to make sure that your appeal follows the guidelines outlined in that document. It will help you understand how to develop and write your appeal so that it can best address the security concerns in your case. Supporting documents should be provided in the order referred to in your written response.

Place your written appeal and supporting documents in a single envelope or package and forward it to the PSAB via the head of your organization. Be sure to sign and date your appeal and submit it within 30 calendar days of your notice of appeal.

C. Appealing with a Personal Appearance

If you choose to have a personal appearance, you must provide DOHA with your request within 10 calendar days of receipt of the LOD. You will receive a notice designating the time, date and place for the personal appearance, which generally with be held within 30 calendar days after your request. The personal appearance generally will be conducted at or near your duty station if it is in the lower 48 states. For people stationed elsewhere, it will be held at or near your duty station or at a DOHA facility in the Washington, D.C. or Los Angeles, California metropolitan area.

At the appearance you will have an opportunity to present oral and documentary information on your own behalf. While the personal appearance is designed so that you can represent yourself, you may obtain legal counsel or other assistance at your own expense to be present at the appearance. If you desire counsel, arrange for it now. Postponement of the personal appearance can be granted only for good cause.

In getting ready for the personal appearance, make sure that you are prepared to address all of the security concerns and supporting adverse information. Also, make sure that your supporting documents are organized and readily accessible for presentation to the AJ presiding at the appearance and for use in answering questions.

The AJ presiding at the appearance will have already reviewed your case file. Therefore, your goal should be to clarify your reasons for overturning the LOD and adding additional information and documentation when appropriate rather than merely to repeat material that you previously submitted. You will not have the opportunity to present or cross-examine witnesses. If you want the views of others presented, make sure that you obtain these views in writing (e.g., letters of reference, letters from medical authorities, etc.) and that you present these documents to the AJ.

During the appearance, you will be allowed to make an oral presentation and submit documentation. You may be asked questions. Answer clearly, completely, and honestly. The AJ is not there to present the government's security concerns but rather to listen to any explanations that you may have concerning your case. This individual did not make the unfavorable personnel security determination set forth in the LOD, and is there to give you an opportunity to present your case as fully as possible.

At the end of the personal appearance, you will be given an opportunity to make a closing statement. You should stress the highlights rather than review your entire case. Try to show how the weight of all available information supports overturning the unfavorable personnel security determination in your case.

The AJ will review the case file, listen to your comments and review any additional documentation that you submit, and then make a recommendation to the PSAB as to whether the clearance, access, or employment in sensitive duties should be denied, revoked or reinstated. The PSAB is not bound by the recommendation of the AJ but will consider it, as well as any additional information you present at your appearance.

AP12. APPENDIX 12

STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD

AP12.1. STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD

Component Personnel Security Appeal Boards (PSABS) shall be structured and function to meet the following requirements:

AP12.1.1. The PSAB will be comprised of three members at the minimum military grade of O-5 or civilian grade of GM/GS-14. In cases where the appellant is at or above the grade of military O-5 or GM/GS- 14, at least one member of the board will be equivalent or senior in grade to the appellant.

AP12.1.2. One of the three members will be a permanent board member and serve as board president. This person should have a thorough knowledge of and experience in the field of personnel security.

AP12.1.3. One of the three members will be an attorney, unless the board has access to legal counsel, and not more than one member shall be from the security career field.

AP12.1.4. The composition of the board may be changed if an appellant works for a Component without a PSAB. A senior official of that Component will be entitled, but not required, to occupy one of the three board positions during consideration of the case.

AP12.1.5. Officials from the Central Adjudication Facility will neither serve as a member of the board nor communicate with board members concerning the merits of an open case.

AP12.1.6. Component PSABs will meet regularly to ensure timely disposition of appeals.

AP12.1.7. Each case shall be reviewed by all three PSAB members. Appeals will be decided by majority vote of the board members present at a meeting to discuss and vote on the case.

AP12.1.8. Component PSABs will render a final determination and notify the individual (via the individual's local organization) in writing. The PSAB will generally notify individuals within 60 calendar days of the receipt of appeal (without personal appearance) or 30 calendar days of receipt of the recommendation of the Administrative Judge (if a personal appearance is requested). This written notification will provide the reasons that the PSAB either sustained or overturned the original determination of the Component Central Adjudication Facility. The PSAB determination will be final and will conclude the appeal process.

AP12.1.9. The PSAB shall maintain a redacted file of all decisions which will be subject to review in accordance with the Freedom of Information Act.

AP13. APPENDIX 13

CONDUCT OF A PERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE (AJ)

AP13.1.1. A person appealing a Letter of Denial (LOD) may request a personal appearance by notifying the Defense Office of Hearings and Appeals (DOHA) in writing at the following address: Director, Defense Office of Hearings and Appeals, Post Office Box 3656, Arlington, Virginia 22203 (FAX No. (703) 696-6865). The request must be sent to DOHA within 10 calendar days of receipt of the LOD. An extension of time may be granted by the Director, DOHA, or designee, for good cause demonstrated by the appellant.

AP13.1.2. Upon receipt of a request for a personal appearance, DOHA shall promptly request the appellant's case file from the appropriate CAF, assign the case to an AJ, and provide a copy of the request to the appropriate PSAB. The CAF shall provide the case file to DOHA normally within 10 calendar days.

AP13.1.3. The AJ will schedule a personal appearance generally within 30 calendar days from receipt of the request and arrange for a verbatim transcript of the proceeding. For appellants at duty stations within the lower 48 States, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location. For individuals assigned to duty stations outside the lower 48 States, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location, or at DOHA facilities located in the Washington, DC metropolitan area or the Los Angeles, California metropolitan area, as determined by the Director, DOHA, or designee.

AP13.1.4. Travel costs for the appellant will be the responsibility of the employing organization.

AP13.1.5. The AJ will conduct the personal appearance proceeding in a fair and orderly manner:

AP13.1.5.1. The appellant may be represented by counsel or personal representative at his own expense;

AP13.1.5.2. The appellant may make an oral presentation and respond to questions posed by his counsel or personal representative, and shall respond to questions asked by the AJ;

AP13.1.5.3. The appellant may submit documents relative to whether the LOD should be overturned;

AP13.1.5.4. The appellant will not have the opportunity to present or cross-examine witnesses;

AP13.1.5.5. Upon completion of the personal appearance, the AJ will generally forward within 30 calendar days, a written recommendation to the appropriate PSAB whether to sustain or overturn the LOD, along with the case file and any documents submitted by the appellant. A copy of the AJ's recommendation will be provided to the CAF.

AP13.1.6. The PSAB will render a final written determination stating its rationale and notify the individual in writing (via the individual's employing organization) generally within 30 calendar days of receipt of the recommendation from DOHA. This decision will be final and will conclude the appeal process.