



# **DEPARTMENT OF DEFENSE**

---

---

# **PERSONNEL SECURITY PROGRAM**

---

---

**June 2002 (Draft)**

**Assistant Secretary of Defense  
For  
Command, Control, Communications, and Intelligence**

## FOREWORD

This Regulation is reissued under the authority of DoD Directive 5200.2, "Defense Personnel Security Program," dated April 9, 1999.

DoD 5200.2-R, "Personnel Security Program Regulation," January 1987, is hereby canceled. DoD Instruction 5210.25, "Assignment of American National Red Cross and United Service Organizations, Inc., Employees to Duty with the Military Services," dated May 12, 1983, and DoD Instruction 5220.28, "Application of Special Eligibility and Clearance Requirements in the SIOP-ESI Program for Contractor Employees," dated March 8, 1978, are hereby canceled and incorporated into this Regulation.

This Regulation applies to the Office of the Secretary of Defense (OSD), the Military Departments (including the Coast Guard when it is operating as a Military Service in the Navy), the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

This Regulation is effective immediately, and is mandatory for use by all DoD Components. The Heads of the DoD Components may issue supplementary instructions only when necessary to provide for unique requirements within their organizations.

Send recommended changes to this Regulation through channels to:

Director, Security  
Office of the Assistant Secretary of Defense for Command,  
Control, Communications, and Intelligence  
6000 Defense Pentagon  
Washington, D. C. 20301-6000

The DoD Components, other Federal Agencies, and the public may download this Regulation from the Washington Headquarters Services web page at <http://www.dtic.mil/whs/directives>.

John P. Stenbit

## TABLE OF CONTENTS

	<u>Page</u>
Foreword .....	2
Table of Contents .....	3
References .....	6
Definitions .....	8
Abbreviations and Acronyms .....	13
 <b>CHAPTER 1 - GENERAL PROVISIONS AND REQUIREMENTS</b>	
C1.1. Purpose and Scope .....	15
C1.2. Program Management .....	15
C1.3. DoD Strategic Timelines .....	17
C1.4. Reports .....	18
C1.5. Inspections .....	18
 <b>CHAPTER 2 – POLICIES</b>	
C2.1. Standards for Access to Classified Information or Assignment to Sensitive Duties .....	19
C2.2. Security Standards .....	19
C2.3. Types and Scope of Personnel Security Investigations (PSIs) .....	21
C2.4. Authorized Personnel Security Investigative Agencies .....	23
C2.5. Limitations and Restrictions .....	27
 <b>CHAPTER 3 - PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS</b>	
C3.1. General .....	30
C3.2. Civilian Employment .....	30
C3.3. Military Service .....	32
C3.4. Security Clearance .....	34
C3.5. Positions Not Requiring Access to Classified Information .....	42
C3.6. Reinvestigation .....	44
C3.7. Authority to Waive Investigative Requirements.....	45
 <b>CHAPTER 4 - ASSOCIATED PROGRAMS</b>	
C4.1. General .....	46
C4.2. Sensitive Compartmented Information (SCI) .....	46
C4.3. Special Access Programs (SAP).....	47

C4.4 Single Integrated Operations Plan–Extremely Sensitive Information (SIOP-ESI).....49

C4.5. Restricted Data and Critical Nuclear Weapons Design Information (CNWDI) .....49

C4.6. Presidential Support Activities .....49

C4.7. Nuclear Weapon Personnel Reliability Program (PRP) .....49

C4.8. Customs Inspectors .....49

C4.9. Persons Requiring Access to Chemical Agents .....49

C4.10. Access to NATO Classified Information .....49

C4.11. Arms, Ammunition and Explosives (AA&E) .....50

C4.12. Contract Linguists .....50

**CHAPTER 5 - RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS**

C5.1. General .....52

C5.2. Prior Personnel Security Investigations .....52

C5.3. Prior Personnel Security Determinations Made By DoD Authorities .....52

C5.4. Investigations Conducted and Clearances Granted by Other Agencies of the Federal Government .....53

**CHAPTER 6 - REQUESTING PERSONNEL SECURITY INVESTIGATIONS**

C6.1. General .....54

C6.2. Authorized Requesters .....54

C6.3. Request Procedures .....55

C6.4. Priority Requests .....55

C6.5. Personal Data provided by the Subject of the Investigation .....55

**CHAPTER 7 - ADJUDICATION**

C7.1. General .....56

C7.2. Central Adjudication .....56

C7.3. Evaluation of Personnel Security Information .....57

C7.4. Adjudicative Record .....58

**CHAPTER 8 - ISSUING CLEARANCES AND GRANTING ACCESS**

C8.1. General.....59

C8.2. Issuing Clearance .....59

C8.3. Granting Access .....60

C8.4. Administrative Withdrawal .....61

CHAPTER 9 - UNFAVORABLE ADMINISTRATIVE ACTIONS

C9.1. Requirements .....62  
 C9.2. Procedures .....63  
 C9.3. Reinstatement of Civilian Employees .....66

CHAPTER 10 - CONTINUING SECURITY RESPONSIBILITIES

C10.1. Evaluating Continued Security Eligibility .....67  
 C10.2. Security Education .....68

CHAPTER 11 - INVESTIGATIVE RECORDS

C11.1. Safeguarding Personnel Security Investigative Records .....70

CHAPTER 12 - AUTOMATED SYSTEMS

C12.1. Defense Clearance and Investigations Index (DCII) .....73  
 C12.2. Joint Personnel Adjudication System (JPAS) .....76

CHAPTER 13 - PEER REVIEW

C13.1. General .....80  
 C13.2. Objectives of Review System .....80  
 C13.3. CAF Participation .....80  
 C13.4. Areas of Review .....80  
 C13.5. Structure of the Review .....81  
 C13.6. Actions as Result of Review .....81

APPENDICES

AP1. Investigative Standards .....82  
 AP2. Request Procedures .....96  
 AP3. Clearance and SCI Access Determination Authorities .....98  
 AP4. Fair Credit Reporting Act Notice and Consent .....100  
 AP5. Adjudicative Guidelines .....103  
 AP6. Information Technology (IT) Positions .....122  
 AP7. List of Sample Notifications .....132  
 AP8. Personnel Security Appeal Board (PSAB) .....150  
 AP9. Investigative Priorities .....151  
 AP10. Personal Appearance .....152  
 AP11. Peer Review .....154

INDEX .....158

## REFERENCES

- (a) Executive Order 12958, "Classified National Security Information", April 17, 1995
- (b) Executive Order 12333, "United States Intelligence Activities", December 4, 1981
- (c) Executive Order 12968, "Access to Classified Information", August 2, 1995
- (d) DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992
- (e) Section 2001 of title 5, United States Code
- (f) Sections 831-835 of title 50, United States Code
- (g) Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953
- (h) DoD Directive 5210.45, "Personnel Security in the National Security Agency", May 9, 1964
- (i) DoD Directive 5100.20, "The National Security Agency and the Central Security Service", December 23, 1971
- (j) DoD Directive 5100.23, "Administrative Arrangements for the National Security Agency," May 17, 1967
- (k) Director of Central Intelligence Directive (DCID) 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," July 2, 1998
- (l) Section 1681 of title 15, United States Code, known as the Fair Credit Reporting Act (FCRA)
- (m) DoD Directive 5105.42, "Defense Security Service (DSS)," May 13, 1999
- (n) "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation," April 5, 1979
- (o) DoD Directive 5210.48, "DoD Polygraph Program," December 24, 1984
- (p) Executive Order 11935, "Citizenship Requirements for Federal Employment," September 2, 1976
- (q) Title 5, United States Code
- (r) Title 10, United States Code
- (s) Title 14, United States Code
- (t) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (u) DoD 5200.1-R, "Information Security Program," January 1997, authorized by DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996
- (v) DoD Directive 5100.3, "Support of the Headquarters of Combatant and Subordinate Joint Commands," November 15, 1999
- (w) DoD Directive 5200.8, "Security of DoD Installations and Resources," April 25, 1991
- (x) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 13, 1997
- (y) DoD Instruction S-5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs) (U)," July 1, 1997
- (z) Section 119e of title 10, United States Code

- (aa) Joint Chiefs of Staff SM (JSCM) 36-76, "Safeguarding the Single Integrated Operational Plan," (U) January 15, 1976
- (bb) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978
- (cc) DoD Directive 5210.55, "Department of Defense Presidential Support Program," December 15, 1998
- (dd) DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program (PRP)," January 8, 2001
- (ee) DoD 5030.49-R, "Customs Inspections," May 1977, authorized by DoD Directive 5030.49, "DoD Customs Inspection Program," January 6, 1984
- (ff) DoD Directive 5210.65, "Chemical Agent Security Program," October 15, 1986
- (gg) 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
- (hh) DoD 5100.76-M, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives," August 12, 2000, authorized by DoD Directive 5100.76, "Physical Security Review Board," February 10, 1981
- (ii) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 1998, authorized by DoD Directive 5400.7, "DoD Freedom of Information Act (FOIA) Program," September 29, 1997
- (jj) DoD 5400.11-R, "Department of Defense Privacy Program," August 1983, authorized by DoD Directive 5400.11, "DoD Privacy Program," December 13, 1999
- (kk) Section 7532 of title 5, United States Code
- (ll) Section 3571 of title 5, United States Code
- (mm) Section 652 (a), (b), and (c) of title 5, United States Code
- (nn) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness and Briefing Program," July 16, 1996
- (oo) Director of Central Intelligence Directive (DCID) 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)," July 20, 1987
- (pp) Section 552a of title 5, United States Code, referred to as the Privacy Act
- (qq) DoD Directive 5105.21, "Defense Intelligence Agency," February 18, 1997
- (rr) Section 1071 of Public Law 106-398, "The Department of Defense Appropriations Act for Fiscal Year 2001," October 30, 2000
- (ss) Section 801 et seq., "Controlled Substances Act," of title 21, United States Code
- (tt) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
- (uu) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
- (vv) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984

## DL1. DEFINITIONS

DL1.1. Access. The ability and opportunity to obtain knowledge of classified information.

DL1.2. Access National Agency Check with Written Inquiries (ANACI). A personnel security investigation for access to classified information conducted by the Office of Personnel Management (OPM), combining a national agency check and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools, and a credit check.

DL1.3. Applicant. A person other than an employee who has an authorized conditional offer of employment for a position that requires access to classified information, or involves the performance of sensitive duties.

DL1.4. Authorized Investigative Agency. An agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information or occupancy of a sensitive position to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information or position.

DL1.5. Central Adjudication Facility (CAF). A single facility designated by the head of the DoD Component to evaluate personnel security investigations and other relevant information

DL1.6. Classified Information. Information that has been determined pursuant to Executive Order (E.O.) 12958 (reference (a)), or any predecessor order to require, in the interest of national security, protection against unauthorized disclosure and has been so designated.

DL1.7. Cohabitant. A person living in a spouse-like relationship with another person.

DL1.8. Condition. See EXCEPTION.

DL1.9. Defense Clearance and Investigations Index (DCII). The DCII is an automated DoD repository that identifies investigations conducted by DoD investigative agencies and personnel security determinations made by DoD adjudicative authorities.

DL1.10. Derogatory Information. Information that could adversely reflect on a person's character, trustworthiness, loyalty, or reliability, for example, a history of drug abuse or criminal activity. Information that is unrelated to character (such as foreign connections) while of adjudicative significance, is not derogatory information. Generally derogatory information is characterized as follows:

DL1.10.1. 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.

DL1.10.2. Significant Derogatory Information. Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

DL1.11. Deviation. See EXCEPTION.

DL1.12. DoD Component. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities.

DL1.13. Electronic Personnel Security Questionnaire (EPSQ). A DoD software program for the preparation and electronic submission of security forms for a personnel security investigation.

DL1.14. Electronic Questionnaire for Investigative Processing (e-QIP). An OPM software program for the preparation and electronic submission of security forms for a personnel security or suitability investigation.

DL1.15. Entrance National Agency Check (ENTNAC). A personnel security investigation scoped and conducted in the same manner as a national agency check on inductees and first-term enlistees into the military. This investigation will be discontinued in FY04.

DL1.16. Exception. An adjudicative decision to grant or continue access eligibility despite a failure to meet adjudicative or investigative standards. Only the head of the agency concerned or designee will make such decisions. An exception precludes reciprocity without review of the case by the gaining organization or program. There are three types:

DL1.16.1. Condition. Access eligibility granted or continued with the proviso that one or more additional measures will be required. Such measures include additional security monitoring, restrictions on access and restrictions on an individual's handling of classified information. Submission of periodic financial statements, admonishment regarding use of drugs or excessive use of alcohol, and satisfactory progress in a government-approved counseling program are examples of conditions.

DL1.16.2. Deviation. Access eligibility granted or continued despite either a significant gap in coverage or scope of investigation or an out-of-date investigation. "Significant gap" for this purpose means either a complete lack of coverage for a period of six months or more within the most recent five years investigated or the lack of an FBI name or technical fingerprint check or the lack of one or more relevant investigative scope components (e.g. employment checks or a subject interview for an SSBI, financial review for any investigation) in its entirety.

DL1.16.3. Waiver. Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. Agency heads or their designees approve waivers only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require special limitations on access, additional security monitoring and other restrictions on the person's handling of classified information beyond normal need-to-know.

DL1.17. Head of DoD Component. The Secretary of Defense; the Secretaries of the Military Departments; the Chairman of the Joint Chiefs of Staff; the Commanders of Combatant Commands; and the Directors of Defense Agencies.

DL1.18. Immediate Family. Mother, father, sister, brother, spouse, son, daughter. Each of these terms includes all its variants; e.g., “sister” includes sister by blood, sister by adoption, half-sister, stepsister, and foster sister. For purposes of determining access eligibility, cohabitants have a status identical to that of immediate family.

DL1.19. 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. (See Temporary Eligibility for Access)

DL1.20. Limited Access Authorization (LAA). Authorization for access to Confidential or Secret information granted to non-U.S. citizens, which is limited to only that information necessary in the course of their assigned duties and releasable under the National Disclosure Policy (NDP).

DL1.21. National Agency Check (NAC). A personnel security investigation consisting of a records review of certain national agencies, including a technical fingerprint search of the files of the FBI.

DL1.22. National Agency Check Plus Written Inquiries (NACI). A personnel security investigation conducted by OPM, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools. All NACI conducted for DoD include a credit check.

DL1.23. National Agency Check with Local Agency Checks and Credit Check (NACLIC). A personnel security investigation covering the past five to seven years and consisting of a NAC, financial review, verification of date and place of birth, and local agency checks.

DL1.24. National Security. The national defense and foreign relations of the United States.

DL1.25. Periodic Reinvestigation (PR). An investigation conducted at prescribed intervals for the purpose of updating a previously completed personnel security investigation or PR.

DL1.26. Personnel Security Determination. A discretionary security decision by appropriately trained adjudicative personnel of all available personal and professional information that bears on the individual’s loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion and sound judgement, as well as freedom from conflicting allegiances and potential for coercion, and the willingness and ability to abide by regulations governing the use, handling and protection of classified information and/or the execution of responsibilities of a sensitive position. Also called security determination.

DL1.27. Personnel Security Investigation (PSI). Any investigation required for 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 conducted for the purpose of making personnel security determinations. They also include investigations of allegations that may arise subsequent to favorable 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.

DL1.28. Scope. The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

DL1.29. Security Clearance. A determination that a person is eligible under the standards of this Regulation for access to classified information. Also called clearance.

DL1.30. Senior Official of the Intelligence Community (SOIC). The heads of organizations within the Intelligence Community as defined by EO 12333 (reference (b)), or their designated representatives.

DL1.31. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical process that is required to be handled within a formal access control system established by the Director of Central Intelligence.

DL1.32. Sensitive Position. Any position 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. The positions covered under this regulation are designated as critical-sensitive or noncritical-sensitive.

DL1.33. Single Scope Background Investigation (SSBI). A personnel security investigation consisting of all of the components prescribed in section I, Appendix A, of this Regulation. The period of investigation for an SSBI is variable, ranging from three years for neighborhood checks to 10 years for local agency checks.

DL1.34. Special Access Program (SAP). A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

DL1.35. 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 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 personnel security determination under the provisions of this Regulation.

DL1.36. Service. Honorable active duty (including attendance at the military academies), membership in the 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 National Industrial Security Program (NISP). Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 24 months.

DL1.37. Temporary Eligibility for Access. Access based on the completion of minimum investigative requirements under exceptional circumstances where official functions must be performed prior to completion of the investigation and adjudication process. Temporary eligibility for access may be granted before the investigations are complete and favorably adjudicated. The Temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation. (See Interim Security Clearance)

DL1.38. Unfavorable Administrative Action. Action taken as the result of an unfavorable personnel security determination as defined in this Regulation.

DL1.39. Waiver. See EXCEPTION.

DL1.40. Unfavorable Personnel Security Determination. A denial or revocation of a security clearance; denial or revocation of access to classified information; denial or revocation of a SAP or SCI access authorization; nonappointment to or nonselection for any 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.

DL1.41. United States Citizen. A person born in one of the following locations is considered to be a United States citizen for personnel security purposes: the 50 United States; the District of Columbia; Puerto Rico; Guam; American Samoa; Northern Mariana Islands; U. S. Virgin Islands; Panama Canal Zone (if the father or mother (or both) was, or is, a citizen of the United States). Individuals born in the Federated States of Micronesia, Marshall Islands, and Palau were previously considered U.S. citizens for personnel security purposes. However, these countries gained their independence and became self-governing on November 3, 1986, October 21, 1986 and October 1, 1994 respectively. Guidance on the legality of grand-fathering citizenship status for these individuals will be inserted later.

## ABBREVIATIONS AND ACRONYMS

AA&E	Arms, Ammunition and Explosives
AJ	Administrative Judge
ANACI	Access National Agency Check With Written Inquiries
ASD	Assistant Secretary of Defense
CAF	Central Adjudication Facility
CI	Counterintelligence
CIA	Central Intelligence Agency
CIPA	Classified Information Procedures Act
COMSEC	Communication Security
CPR	Confidential Periodic Reinvestigation
CSA	Cognizant Security Authority
DAS	Disclosure Accounting System
DASD(S&IO)	Deputy Assistant Secretary of Defense (Security & Information Operations)
DCID	Director of Central Intelligence Directive
DCII	Defense Clearance and Investigations Index
DMDC	Defense Manpower Data Center
DIA	Defense Intelligence Agency
DSS	Defense Security Service (Formerly Defense Investigative Service)
DISCO	Defense Industrial Security Clearance Office
DoD	Department of Defense
DOHA	Defense Office of Hearings and Appeals
DOS	Department of State
DPOB	Date and Place of Birth
E.O.	Executive Order
ENTNAC	Entrance National Agency Check
EOD	Explosive Ordnance Disposal
EPSQ	Electronic Personnel Security Questionnaire
e-QIP	Electronic Questionnaire for Investigative Processing
ES	Executive Service
FBI	Federal Bureau of Investigation
FBI-HQ/ID	Federal Bureau of Investigation-Headquarters/Identification
INS	Immigration and Naturalization Service
JCS	Joint Chiefs of Staff
LAA	Limited Access Authorization
LOCN	Letter of Compelling Need
LOD	Letter of Denial
MOU	Memorandum of Understanding
NAC	National Agency Check
NACI	National Agency Check With Written Inquiries
NACLC	National Agency Check With Local Agency Checks & Credit Checks
NATO	North Atlantic Treaty Organization
NISP	National Industrial Security Program

OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PAR	Program Access Request
POC	Point of Contact
PR	Periodic Reinvestigation
PRP	Personnel Reliability Program
PSAB	Personnel Security Appeals Board
PSI	Personnel Security Investigation
PSQ	Personnel Security Questionnaire
ROTC	Reserve Officers Training Corps
SAP	Special Access Program
SAPCO	Special Access Program Coordination Office
SAPOC	Special Access Program Oversight Committee
SCI	Sensitive Compartmented Information
SII	Special Investigative Inquiry
SIOP-ESI	Single Integrated Operations Plan - Extremely Sensitive Information
SOIC	Senior Officials of the Intelligence Community
SOR	Statement of Reasons
SPR	SECRET Periodic Reinvestigation
SSBI	Single Scope Background Investigation
SSN	Social Security Number
USO	United Service Organization
USSAN	United States Security Authority for NATO Affairs
WHS	Washington Headquarters Services

## C1. CHAPTER 1

### GENERAL PROVISIONS AND REQUIREMENTS

#### C1.1. PURPOSE AND SCOPE

C1.1.1. This Regulation implements E.O.12968 (reference (c)), which established a uniform Federal personnel security program for initial or continued access to classified information.

C1.1.2. This Regulation establishes policies and procedures to ensure that acceptance and retention of DoD military personnel and civilian employees and granting them, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security. It sets forth standards, criteria and guidelines upon which personnel security determinations shall be based and prescribes the kinds and scopes of personnel security investigations required for access to classified information or placement in sensitive positions. It also details the procedures by which personnel security determinations shall be made and appealed and delineates program management responsibilities.

C1.1.3. This Regulation applies to all DoD Components, DoD contractor personnel and other personnel affiliated with the Department of Defense, except that the unfavorable administrative procedures pertaining to contractor personnel requiring access to classified information are contained in DoD Directive 5220.6 (reference (d)).

C1.1.4. Under combat conditions or other military exigencies, an authority in Appendix 3 may waive such provisions of this Regulation as the circumstances warrant.

#### C1.2. PROGRAM MANAGEMENT

C1.2.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) has been designated by the Secretary of Defense as the senior official responsible for the direction and administration of the Personnel Security Program for the Department of Defense. The ASD(C3I) shall:

C1.2.1.1. Provide program management through issuance of policy and operating guidance.

C1.2.1.2. Serve as the senior DoD official responsible for oversight implementation of SCI security policies and procedures within the DoD.

C1.2.1.3. Serve as the senior DoD official responsible for administering that portion of the DoD Personnel Security Program pertaining to DoD Special Access Programs (SAPs).

C1.2.2. The Deputy Assistant Secretary of Defense for Security and Information Operations (DSAD(S&IO)). The ASD(C3I) has designated the DASD(S&IO) as the Department's focal point for personnel security matters within the Department. The DASD(S&IO) shall:

C1.2.2.1. Provide staff assistance to the DoD Components in resolving day-to-day security policy and operating problems.

C1.2.2.2. Issue policy guidance, interpretation, and clarification as needed.

C1.2.2.3. Conduct inspections of the DoD Components for implementation and compliance with DoD security policy and operating procedures.

C1.2.2.4. Provide policy, oversight, and guidance to the Component adjudication functions.

C1.2.2.5. Approve, coordinate and oversee all DoD personnel security research initiatives and activities.

C1.2.3. DoD General Counsel.

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 persons 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.

C1.2.4. DoD Components. The Heads of each DoD Component shall:

C1.2.4.1. Commit necessary resources for the effective implementation of the Personnel Security Program.

C1.2.4.2. Establish a mechanism to accurately project personnel security investigative workload requirements each year.

C1.2.4.3. Ensure applicable personnel security requirements are included in all contracts, agreements, memorandums of understanding, and other similar instruments.

C1.2.4.4. Appoint a Senior Official to be responsible for direction and administration of the personnel security program within the Component. The Senior Official shall:

C1.2.4.4.1. Oversee the Personnel Security Program within the Component.

C1.2.4.4.2. Issue (or cause to be issued) implementing directives as necessary for program implementation.

C1.2.4.4.3. Establish and maintain an ongoing self-inspection program to include periodic review and assessment of workload requirements and processes, and adjudicative functions (if applicable).

C1.2.4.4.4. Ensure that the performance contract or other system used to rate the performance of civilian and military personnel include a comment regarding the employee's discharge of security responsibilities under the Component guidance.

C1.2.4.4.5. Ensure prompt and appropriate response to any request, appeal, challenge, compliant, or suggestion arising out of the implementation of this Regulation within the Component, and

C1.2.4.4.6. Ensure prompt response to requests from ASD(C3I), DASD(S&IO) and General Counsel concerning any aspect of this program.

C1.2.5. The policies and procedures, which govern the National Security Agency/Central Security Service, are prescribed by 5 U.S.C., 50 U.S.C., E.O. 12333 and 10450, DoD Directives 5210.45, 5100.20 and 5100.23, and DCID 6/4 (references (e), (f), (b), (g), (h), (i), (j), and (k) respectively).

### C1.3. DoD STRATEGIC TIMELINES

C1.3.1. The Department has established the following timelines to ensure an efficient and effective personnel security program. Investigative and adjudicative actions are to be completed as follows:

C1.3.1.1. Investigative. Timelines are based on average case times

C1.3.1.1.1. NACLCLC – 75 days

C1.3.1.1.2. SSBI – 90 days

C1.3.1.1.3. SSBI-PR – 120 days

C1.3.1.1.4. NACLCLC-PR – 120 days

C1.3.1.1.5. SII – 90 days

C1.3.1.2. While timely completion of investigations can be dependent upon other activities or agencies, the investigative provider is obligated to make every effort to meet the above timelines. The investigative provider in conjunction with these other agencies and activities shall continually seek ways to improve timely receipt of investigative information.

C1.3.1.3. Adjudicative. Cases are to be adjudicated within 30 days of receipt. Cases requiring a statement of reasons or other administrative actions should be processed as expeditiously as possible.

#### C1.4. REPORTS

The Joint Personnel Adjudication Systems (JPAS) and the Defense Manpower Data Center (DMDC) will be the primary databases used by DASD(S&IO) to obtain personnel security program management data on a fiscal year basis. This information is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and the Congress. The data shall include the number of personnel holding clearances within the DoD, the number of clearances issued, denied, or revoked each fiscal year, the number of investigations conducted each year as well as timeliness of those investigations and other program management data as needed.

#### C1.5. INSPECTIONS

Heads of DoD Components shall establish and maintain a self-inspection program to evaluate and assess the effectiveness and efficiency of the Component's implementation of the DoD Personnel Security Program. The program shall also include the effectiveness and efficiency of services provided (if applicable) to other DoD Components.

## C2. CHAPTER 2

### POLICIES

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

C2.1.1. Only United States citizens shall be granted a security clearance, assigned to sensitive duties, or granted access to classified information.

C2.1.2. The Department of Defense does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information or assignment to sensitive duties.

C2.1.3. For the purposes of this Regulation, it is not necessary for the performance of duties to involve classified activities or classified matters in order for the duties to be considered sensitive and/or critical to the national security. An investigation may be required to provide assurance that personnel in these positions are reliable and trustworthy.

C2.1.4. Objective of the Personnel Security Program. The objective of the personnel security program is that military, civilian, and contractor personnel assigned to and retained in sensitive positions, in which they could potentially damage national security, are and remain reliable and trustworthy, and there is no reasonable basis for doubting their allegiance to the United States.

C2.1.5. Clearance and Sensitive Position Standard. The standard is whether the facts and circumstances indicate 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 national security interests of the United States.

C2.1.6. Military Service Standard. No person who has been convicted of a felony, unless an exception in meritorious cases has been authorized, or previously separated from the Armed Forces under conditions other than honorable or for the good of the service, or disqualified under the moral standards of acceptability for service shall be appointed, enlisted, inducted or retained in the Armed Forces.

#### C2.2. SECURITY STANDARDS

C2.2.1. Criteria for Application of Security Standards. These standards shall be the basis for all personnel security determinations. These determinations shall be based upon careful consideration of the following adjudicative issues and their security concerns, each of which is to be evaluated in the context of the whole person, as explained in Appendix 5:

C2.2.1.1. Allegiance 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.

C2.2.1.2. 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 not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

C2.2.1.3. Foreign preference. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

C2.2.1.4. Sexual behavior. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. 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.

C2.2.1.5. Personal conduct. Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

C2.2.1.6. 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.

C2.2.1.7. 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.

C2.2.1.8. 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.

C2.2.1.9. 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.

C2.2.1.10. Criminal conduct. A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

C2.2.1.11. Security violations. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness and ability to safeguard classified information.

C2.2.1.12. Outside activities. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

C2.2.1.13. 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, transmission, processing, manipulation, and storage of classified or sensitive information.

### C2.3. TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS (PSIs)

C2.3.1. General. The types of PSIs authorized herein 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 DASD(S&IO).

C2.3.2. National Agency Check (NAC). A NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making personnel security determinations. A NAC is also an integral part of all initial and periodic reinvestigations and is the baseline for trustworthiness determinations.

C2.3.3. Access National Agency Check plus Written Inquiries (ANACI). The ANACI is the investigative requirement for federal employees under E.O. 10450 (reference (g)) in non-critical sensitive positions that require access to classified information up to the Secret level. The ANACI is conducted by OPM. It consists of a NAC, written inquiries and record searches which includes coverage of law enforcement agencies, former employers and supervisors, references, schools and finances covering the last five to seven years.

C2.3.4. National Agency Check plus Written Inquiries (NACI). The NACI is the baseline investigative requirement for entry into government service under E.O. 10450 (reference (g)) and for federal employees in positions that do not require access to classified information. It is conducted by OPM. The NACI consists of a NAC, written inquiries and record searches which includes coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last five years. All OPM NACI conducted for DoD includes a credit check.

C2.3.5. National Agency Check With Local Agency Checks & Credit Checks (NACLCL). The NACLCL is the prescribed investigation for initial and continued access to Secret and Confidential information for DoD military and contractor personnel. It is also the reinvestigation requirement for federal employees at the same access levels. Scope of the NACLCL is found in Appendix 1.

C2.3.6. Single Scope Background Investigation (SSBI). The SSBI is the initial investigation for access to Top Secret (including Top Secret Special Access Programs (SAPs)), Sensitive

Compartmented Information (SCI), and for Critical Sensitive Positions. Its scope is detailed in Appendix 1.

C2.3.7. Special Investigative Inquiry (SII). SII is a PSI conducted to prove or disprove allegations relating to the security standards outlined in section C2.2. SII is 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. 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.

C2.3.8. Periodic Reinvestigation (PR). Certain categories of duties, clearance, and access require a PR. A PR is conducted at intervals of 5, 10 or 15 years. PR scopes are outlined in Appendix 1.

C2.3.9. Subject Interview. Investigative experience and analysis over the years has demonstrated that, the subject of a personnel security investigation is frequently the best source of accurate and relevant information concerning the matters under consideration. Further, Privacy Act provisions 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, subject 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 subparagraphs.

C2.3.9.1. SSBI and SSBI/PR Trained security, investigative or counterintelligence personnel shall conduct a subject interview as part of each SSBI and SSBI/PR.

C2.3.9.2. Resolving Adverse Information. A personal interview of the subject may be conducted by trained security, investigative, or counterintelligence personnel, when necessary, as part of each SII, as well as during the course of initial or expanded investigations, to resolve or clarify any information that may impugn the subject's moral character, threaten the subject's future Federal employment, raise the question of subject's security eligibility, or be otherwise stigmatizing.

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

#### C2.3.11. Fair Credit Reporting Act (FCRA)

C2.3.11.1. Amendments to the FCRA (reference (1)) expanded the obligations and responsibilities of employers with respect to obtaining and using "consumer reports." The amendments require individuals be notified that credit reports may be obtained for employment purposes; that written consent is obtained before such reports are procured; and that individuals are notified promptly if information in their credit report may result in an adverse employment (or security clearance) determination.

C2.3.11.2. This applies to any investigation initiated on DoD military, civilian or contractor personnel using Standard Forms (SF) 86 (Questionnaire for National Security Positions), 85P (Questionnaire for Public Trust Positions) or 85 (Questionnaire for Non-Sensitive Positions) that includes a credit bureau check. The release form that is part of the SF86, 85P and 85 will not suffice for this purpose.

C2.3.11.3. Before an individual's credit report is obtained for employment or security clearance purposes, the individual must first be notified in writing, in a document consisting solely of the notice that a credit report may be obtained for such purposes. Appendix 4 contains the notice that must be provided to all military, civilian or contractor personnel when they are asked to complete a SF86, 85P, or 85. Investigations that do not normally include a credit check, like a NAC or ENTNAC are not part of this requirement.

C2.3.11.4. The individual's written authorization must also be obtained before a credit bureau report may be requested. Appendix 4 contains the consent form that must be completed by all personnel who will be the subject of an investigation that includes a credit bureau check. If the individual receives the disclosure notice and provides written permission to obtain reports during the course of his and her employment with DoD, no further notice or permission is required before future reports are obtained for employment (security clearance) purposes. If the individual declines to provide written authorization, the investigation will be discontinued. The DoD Component shall initiate action to deny or revoke the security clearance of the individual or employment in a sensitive position.

C2.3.11.5. DoD will use the disclosure notice and consent form to obtain consumer credit reports to make determinations regarding employment, including military accessions, retention in sensitive positions, or eligibility for access to classified information. The notice and consent forms will be retained by the individual's security office for as long as the person is employed or assigned to the agency, activity, organization, or contractor.

C2.3.11.6. The amendments to the FCRA require that if an adverse action is going to be taken in whole or in part based on the credit report, a copy of the report must be furnished to the individual and a written description of the rights of the consumer under this title. No further notice will be required under this section of the FCRA when the due process and appeal procedures contained in this Regulation and DoD Directive 5220.6 (reference (d)) are used when a clearance is denied or revoked or a person is denied employment in a sensitive position.

#### C2.4. AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES

C2.4.1. The Defense Security Service (DSS) and OPM, hereafter referred to as investigative provider, unless specifically delineated, are the investigative providers for conduct of personnel security investigations for DoD within the fifty states, the District of Columbia, and the Commonwealth of Puerto Rico. (See DoD Directive 5105.42, (reference (m)) and E.O. 10450 (reference (g)), except as provided for in DoD Directive 5100.23 (reference (j))). DSS will act as the conduit to request the Military Departments to accomplish DoD investigative requirements in geographic areas serviced by the Military Departments outside of the United States. The investigative provider will request, as required, assistance from other appropriate Federal

Agencies to accomplish DoD investigative requirements in other geographic areas beyond their jurisdiction. No other DoD Component shall conduct, or contract for the conduct of personnel security investigations unless specifically authorized by DASD(S&IO). In certain instances provided for below, a personnel security investigation shall be referred to other investigative agencies.

#### C2.4.2. Allegiance to the United States

C2.4.2.1. In the context of DoD investigative policy, this section 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.

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 and/or Federal Bureau of Investigation (FBI) Jurisdiction. Allegations of activities covered by criteria in subparagraphs C2.2.1.1. through C2.2.1.3. are the primary responsibility 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 (n)). Whenever allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a PSI conducted by an authorized investigative provider, they shall be referred immediately to either the FBI or to a Military Department counterintelligence agency as appropriate.

C2.4.2.3. Allegations of activities limited to those set forth in subparagraphs C2.2.1.4. through C2.2.1.13. shall be investigated by an authorized investigative provider.

#### C2.4.3. Suitability Information

C2.4.3.1. Most derogatory information developed through personnel security investigations is suitability information; that is, information pertaining to activities or situations covered by subparagraphs C2.2.1.4. through C2.2.1.13. Almost all unfavorable personnel security determinations made by DoD authorities are based on derogatory suitability information, although such information may be used as a basis for unfavorable administrative actions not of a

security nature, such as action under the Uniform Code of Military Justice (UCMJ) or removal from Federal employment under OPM regulations.

C2.4.3.2. Pre-clearance Investigation. Derogatory suitability information, except that covered in subparagraph C2.4.3.4. developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel security clearance, shall be investigated to the extent necessary to confirm or refute its applicability to criteria in paragraphs C2.2.1.4. through C2.2.1.13.

C2.4.3.3. Post-adjudicative Investigation. Derogatory suitability allegations, except those covered by C2.4.3.4. which arise subsequent to clearance and require investigation to resolve as well as to determine an employee's eligibility for continued access to classified information, reinstatement of clearance and/or access, or retention in a sensitive position shall be the subject of an SII. Reinvestigation of employees for adjudicative reconsideration due to the passage of time (no sooner than 12 months from the final personnel security determination) or evidence of favorable behavior shall also be referred for investigation. In such cases, completion of appropriate security forms by the subject constitutes consent to be investigated. If subject has not terminated DoD affiliation and/or has retained access to classified information, individual consent or completion of an investigative form is not required when subparagraph C3.6.1.4. applies. Post-adjudication investigation of allegations of a suitability nature required to support other types of unfavorable personnel 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 the investigative provider.

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 DoD criminal investigative agency, Military Department or civilian jurisdiction unless the limitations in subparagraphs C2.4.3.4.1. through C2.4.3.4.3., apply. Where the allegation concerns a potential violation of the UCMJ, 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 of 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 CAFs) for any purpose. That limitation does not apply to allegations that a person attempted, solicited, or committed a criminal offense of a sexual nature 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 person.

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 designee.

C2.4.3.4.3. Information about a person's sexual orientation or statements by a person 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 CAFs) for any purpose. If investigative reports containing such information are referred to law enforcement agencies or Military Departments for other reasons, such information will be removed.

#### C2.4.4. Foreign Influence

C2.4.4.1. When a member of subject's immediate family or such other person to whom the person is bound by obligation or affection resides in a country whose interests may be inimical to the interests of the United States, further investigation may be warranted. The rationale underlying this category of investigation is based on the possibility that a person in such a situation might be coerced, influenced, or pressured to act contrary to the interests of national security.

C2.4.4.2. When there are indications that a foreign intelligence service is taking action specifically directed against the person, or there is other evidence that the person is actually being coerced, influenced, or pressured by a foreign government, the case becomes a counterintelligence matter outside the investigative jurisdiction of the investigative provider. The case shall be referred to the appropriate Military Department or the FBI.

C2.4.4.3. In the absence of evidence of any coercion, influence or pressure, foreign interest investigations are exclusively a personnel security matter, rather than counterintelligence. The investigative provider shall conduct these investigations.

C2.4.5. Overseas Personnel Security Investigations. PSIs requiring overseas leads shall be conducted, under the direction and control of DSS, except as provided for in DoD Directive 5100.23 (reference (j)), by the appropriate Military Department investigative organization. Only

post-adjudication and LAA 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 with a copy of the investigative request sent to the investigative provider. In such cases, the Military Department investigative agency will complete the investigation and forward the completed report of investigation directly to the investigative provider, with a copy to the requester.

## C2.5. LIMITATIONS AND RESTRICTIONS

C2.5.1. Authorized Requesters of Personnel Security Investigations. Only those authorities designated in Chapter 6 may request PSIs.

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 operational requirements. Special attention shall be given to eliminating unnecessary or duplicative clearances and requests for PSIs.

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 PSI. Such additional information required to make the necessary personnel security determination shall be obtained as appropriate from knowledgeable personal sources, particularly subject's 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 a person preparatory to the initiation of a PSI, the person must be informed of (a) the authority (statute or Executive Order that authorized solicitation); (b) the principal purpose or purposes for which the information is to be used; (c) the routine uses to be made of the information; (d) whether furnishing such information is mandatory or voluntary; (e) the effect on the person, if any, of not providing the information; and (f) that subsequent use of the data may be employed as part of an aperiodic, 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 or mental health should be limited to only those areas that are relevant to the criteria of section C2.2. of this Chapter. Similarly, the probing of a person's thoughts or religious and political beliefs, and questions about conduct that have no personnel security implications, are not authorized by this Regulation. When conducting investigations under the provisions of this Regulation, investigators shall:

C2.5.5.1. Investigate only those persons whose cases are officially assigned to the investigator.

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 subject's right to obtain the information provided by the sources and to learn the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisement to subjects of PSIs are outlined in subparagraph C2.5.4. of this Chapter.

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, deceptive 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 and her fairness, impartiality, or objectivity.

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

C2.5.5.8. Refrain from attempting to evaluate material contained in medical files. Only such personnel designated by DoD medical authorities shall evaluate medical files for personnel security program purposes. However, authorized investigative personnel may accomplish review and collection of medical record information.

C2.5.5.9. Telephone Interview Policy. Personal interviews are the preferred means of conducting an investigation. However, use of the telephone in certain circumstances may be warranted. Telephone interviews are permitted under the following conditions:

C2.5.5.9.1. Telephone interviews shall not exceed 10% of the interviews in an investigation.

C2.5.5.9.2. The reference or record custodian requests a telephone interview. Investigators are prohibited from coaxing or persuading an interviewee to ask for a telephonic interview or offering the option of being interviewed over the telephone.

C2.5.5.9.3. An established relationship exists between the investigator and the other party.

C2.5.5.9.4. Situations prevailing in a specific locale where safety of the investigator may be placed in jeopardy.

C2.5.5.9.5. Situations necessitated by exigency; e.g. when the area is too remote, or when climate conditions render travel impossible. Use of the telephone to complete an overdue investigation is permitted when it can be accomplished without compromising quality, but only in rare circumstances. This is not an exigency. Proper planning should make use of the telephone an exception.

C2.5.5.9.6. A record repository request that record searches be conducted by telephone or by facsimile (fax).

C2.5.5.9.7. Telephone interviews are not permitted on investigations with significant issues. Telephone interviews on investigations with minor issues are permissible, though not the preferred investigative method and should be used with extreme discretion.

C2.5.5.9.8. All telephone interviews will be documented and the reason(s) why.

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 (o)).

### C3. CHAPTER 3

#### PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

##### C3.1. GENERAL

This Chapter outlines the investigative requirements for government employment, placement in sensitive positions, entry into military service, access to classified information, trustworthiness determinations and reinvestigations.

##### C3.2. CIVILIAN EMPLOYMENT

C3.2.1. Per E.O. 10450 (reference (g)), all persons employed in the departments and agencies of the Government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his and her department or agency an effective program to ensure that the employment and retention of any civilian officer or employee is clearly consistent with the interests of national security. Additionally, the head of each agency shall designate or cause to be designated as a sensitive position, any position in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on the national security. Non-U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by OPM pursuant to E.O. 11935 (reference (p)). Exceptions to these requirements shall be permitted only for compelling national security reasons. A synopsis of the sensitivity level designations and investigative requirements for civilian employees within the Department of Defense is provided for ease of reference. However, appropriate directives and publications regarding civilian employment within DoD and OPM issuance should be consulted for definitive guidance.

##### C3.2.2. Sensitive Positions

C3.2.2.1. The Heads of DoD Components or designee(s) shall designate each position within their jurisdiction as to its security sensitivity. These designations should be periodically reviewed for currency vis-à-vis the specific duties of each position, and held to a minimum consistent with mission requirements. It is important that only positions that truly meet one or more of the criteria set forth in this Chapter be designated as sensitive.

C3.2.2.2. Each civilian position shall be designated as Critical-sensitive or Noncritical-sensitive. The criteria to be applied in designating a position as sensitive are:

C3.2.2.2.1. Critical-Sensitive (CS). Any position that has the potential for exceptionally grave damage to the national security. Includes positions involving any of the following:

C3.2.2.2.1.1. Access to TOP SECRET information.

C3.2.2.2.1.2. Development or approval of war plans, plans or particulars of future or major or special operations of war, or critical and extremely important items of war;

C3.2.2.2.1.3. Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, rendering of personnel security determinations, or duty on personnel security boards; or

C3.2.2.2.1.4. Other positions related to national security, regardless of duties, that requires the same degree of trust.

C3.2.2.2.2. Noncritical-Sensitive (NCS). Any position with potential for some damage to serious damage to the national security. Includes positions involving any of the following:

C3.2.2.2.2.1. Access to SECRET or CONFIDENTIAL national security materials or information, etc.

C3.2.2.2.2.2. Duties that may directly or indirectly adversely affect the national security operations of the agency.

C3.2.2.2.2.3. Any other position so designated by the Head of the DoD Component or designee.

### C3.2.3. Investigative Requirements

C3.2.3.1. The appointment of each civilian employee in any DoD Component is subject to investigation, except for reappointment when the break in service is less than 24 months. The type of investigation required is set forth according to position sensitivity.

#### C3.2.3.2. Noncritical-Sensitive Positions

C3.2.3.2.1. A NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical-sensitive position (for exceptions see subparagraph C3.2.5. below). An ENTNAC, NAC or NACLC conducted during military or contractor employment may also be used for appointment provided a NACI or ANACI (if access to classified information is required) has been requested from OPM and there is no more than 24 months break in service.

C3.2.3.2.2. Although seasonal employees (including summer hires) normally do not require access to classified information, a NACI is the minimum investigative requirement for all such employees in noncritical-sensitive positions. For those that require access to classified information the appropriate, higher level investigation is required. The request for the NACI should be submitted to OPM, in accordance with OPM processing guidelines, within 3 workdays after a person is appointed to these positions.

### C3.2.3.3. Critical-Sensitive Positions

An SSBI shall be initiated prior to appointment to critical-sensitive positions (for exceptions see subparagraph C3.2.5.). The investigative provider as appropriate will conduct SSBI.

### C3.2.3.4. Exceptions to Investigative Requirements

C3.2.3.4.1. Noncritical-Sensitive. A noncritical-sensitive position may be occupied pending the completion of the NACI or ANACI 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 or ANACI has been requested.

C3.2.3.4.2. Critical-Sensitive. A critical-sensitive position may be occupied pending completion of the SSBI 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 SSBI or a previous valid NACI, NAC, NACL or ENTNAC has been completed and favorably adjudicated, and there is no more than 24 months break in service since completion of the investigation.

C3.2.4. Periodic reinvestigation (PR) requirements. The head of each agency is responsible for ensuring the retention in employment of civilian employees within the agency is clearly consistent with the interests of national security. To further this intent, civilian personnel in sensitive positions in the Department of Defense are subject to a PR as follows:

C3.2.4.1. Critical-Sensitive Positions. Each DoD civilian employee occupying a critical-sensitive position shall undergo a PR conducted on a five year recurring basis scoped as set forth in Standard C, Appendix 1.

C3.2.4.2. Noncritical-sensitive Positions. Heads of DoD Components may establish PR requirements for noncritical-sensitive positions. These investigations will be conducted on a ten year recurring basis scoped in accordance with Standard A, Appendix 1.

C3.2.5. Mobilization of DoD Civilian Retirees. The requirements contained in subparagraph C3.2.3. about the type of investigation required by position sensitivity for DoD civilian retirees temporary appointment when the break in service is greater than 24 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of Title 5 U.S.C. (reference (q)), depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to personnel assigned to the DoD intelligence and security agencies with respect to granting security clearances in an expeditious manner under subparagraph C3.2.3.

## C3.3. MILITARY SERVICE

C3.3.1. 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 PSI. The types of investigation required are set forth below.

### C3.3.2. Entrance Investigation

C3.3.2.1. A NACLCL<sup>1</sup> is required for entry into the Armed Forces, active duty, guard, or reserve. It shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. Further, NACLCL shall be conducted on each commissioned officer (except as permitted by section C.4.), warrant officer, cadet, midshipman, and Reserve Officers Training Corps (ROTC) candidate, at the time of appointment. A NACLCL shall be conducted upon reentry of any of the above when there has been a break in service greater than 24 months.

C3.3.2.2. If an officer or warrant officer candidate has been the subject of a favorable NACLCL and there has not been a break in service of more than 24 months, a new NACLCL 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 appointment process that results in a moral waiver is to be fully explained in a written summary attached to the SF 86.

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: Health professionals, chaplains, and attorneys may be commissioned in the Reserve components prior to completion of a NACLCL provided that:

C3.3.4.1. A NACLCL 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 and 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 non-U.S. citizen health professionals, chaplains, and attorneys.

C3.3.5. Mobilization of Military Retirees. The requirements contained in paragraph C3.3.2.1., should be waived for the purposes of partial or full mobilization under 10 U.S.C. (reference (r)), or 14 U.S.C. (reference (s), pertaining to the U.S. Coast Guard as an element of the Navy), to include the period of prescribed service refresher training. Priority should be afforded to military retirees mobilized and assigned to the DoD intelligence and security communities.

---

<sup>1</sup> NACLCL will replace ENTNAC as the baseline investigation for entry into the military service (active duty, guard, reserve) beginning FY04.

## C3.4. SECURITY CLEARANCE

### C3.4.1. General

C3.4.1.1. The authorities designated in Appendix 3 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 to perform or assist in a lawful and authorized governmental function.

C3.4.1.2. Personnel who are employed by or serving in a military, civilian, contractor or 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 personnel may be granted either a final or interim personnel security clearance provided the investigative requirements set forth herein are met, and all available information has been favorably adjudicated.

### C3.4.2. Investigative Requirements for Clearance

#### C3.4.2.1. Top Secret

##### C3.4.2.1.1. Final Clearance: SSBI

##### C3.4.2.1.2. Interim Clearance

C3.4.2.1.2.1. As a minimum: Favorably completed NAC.

C3.4.2.1.2.2. Favorable review of SF-86.

C3.4.2.1.2.3. SSBI 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. Provisions of subparagraph C3.2.3.4. have been met regarding civilian personnel.

#### C3.4.2.2. Secret and Confidential

##### C3.4.2.2.1. Final Clearance:

C3.4.2.2.1.1. NACLIC: Military personnel and contractor employees.

C3.4.2.2.1.2. ANACI: Civilian employees.

##### C3.4.2.2.2. Interim Clearance:

C3.4.2.2.2.1. Favorable review of SF-86.

C3.4.2.2.2.2. NACLC or ANACI initiated.

C3.4.2.2.2.3. Favorable review of local personnel, base and/or military police, medical, and security records as appropriate.

C3.4.2.2.2.4. Provisions of subparagraph C3.2.3.4. have been complied with regarding civilian personnel.

C3.4.3. Validity of Previously Granted Clearances. Clearances previously granted under less stringent investigative requirements retain their validity but must comply with the prevailing periodic reinvestigation interval. However, if a higher degree of clearance is required, investigative requirements of this Regulation shall be followed.

C3.4.4. Access to Classified Information by Non-U.S. Citizens

C3.4.4.1. Only U.S. citizens are eligible for a security clearance. However, compelling reasons may exist for granting access to classified information to a non-U.S. citizen. A Limited Access Authorization (LAA) may be granted in those rare circumstances where the non-U.S. citizen possesses unique or unusual skill or expertise that is needed to support a specific U.S. Government contract and a cleared or clearable U.S. citizen is not available.

C3.4.4.2. Access to classified or controlled unclassified information provided by another government or international organization shall not be permitted under a LAA without written consent of the government or organization that provided the information.

C3.4.4.3. Limitations

C3.4.4.2.1. 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 cleared or clearable U.S. citizen.

C3.4.4.2.2. 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.

C3.4.4.2.3. LAA personnel shall not be designated as courier or escort for classified material outside the location in which access is permitted unless they are accompanied by an appropriately cleared U.S. citizen.

C3.4.4.3. Authorized Access Levels

C3.4.4.3.1. LAAs may be granted only at the SECRET and CONFIDENTIAL levels. LAAs for higher level access are prohibited. Interim access may be granted following

completion of the SSBI, by an authority in Appendix 3 and compliance with the requirement in subparagraph C3.4.4.4.1.

C3.4.4.3.2. The classified information to which the non-U.S. citizen may have access must be approved for release to the person's country (or countries) of citizenship, in accordance with DoD Directive 5230.11 (reference (t)).

C3.4.4.3.3. Access to classified information shall be limited or related to a specific program or project. The LAA shall be canceled upon completion of the program or project for which it was approved, or rejustified as described herein.

C3.4.4.3.4. 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 (u)).

#### C3.4.4.4. Requirements

C3.4.4.4.1. When a non-U.S. citizen 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 country's investigative requirements, which are commensurate with the standards provided herein, an LAA may be issued at the requisite level. Non-US citizens will not be eligible for access to any greater level of classified information than the U.S. Government has determined may be released to the country of which the person is a citizen.

C3.4.4.4.2. In addition to the above, a favorably completed (within the last five 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 (o))) must be favorably completed before granting access.

C3.4.4.4.3. If geographical, political or medical situations prevent the full completion of the SSBI or prevent the polygraph examination to supplement a less than full SSBI, an LAA may be granted only with approval of DASD(S&IO).

C3.4.4.4.4. If an LAA is withdrawn and the person subsequently is considered for an LAA, an SSBI and polygraph examination may be required. The scope of the SSBI normally shall cover the period since the previous investigation or ten years, whichever is shorter.

C3.4.4.4.5. A PR shall be conducted on every person with an LAA five years from the date of the prior SSBI or PR, as appropriate.

C3.4.4.4.6. All requests for initial LAAs shall contain a detailed justification and technical control plan describing the following:

C3.4.4.4.6.1. Location of the classified material in relationship to the location of the non-U.S. citizen.

C3.4.4.4.6.2. Compelling reason for not employing a cleared or clearable U.S. citizen.

C3.4.4.4.6.3. Synopsis of an annual continuing assessment program to evaluate the individual's continued trustworthiness and eligibility for access.

C3.4.4.4.6.4. Plan to control access to secure areas and to classified and controlled unclassified information.

#### C3.4.4.5. LAA Determination Authority

C3.4.4.5.1. LAA determinations may only be made by an official listed in Appendix 3. The designated single authorizing official for the Military Departments, the Combatant Commands, and the DSS precludes issuance of a final LAA determination by any other official at the major command level, or equivalent.

C3.4.4.5.2. LAA determinations for employees of the Military Departments shall be the sole authority of the Secretary of the Military Department or single designee such as the Service CAF. Field elements must submit their recommendations for access to the designated official for approval, along with information to support the action.

C3.4.4.5.3. The Commander of a Combatant Command, or single designee (flag or general 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 CAF of the Military Department in accordance with the assigned responsibilities in DoD Directive 5100.3 (reference (v)) for inclusion in the JPAS.

C3.4.4.5.4. All LAA determinations, favorable and unfavorable, shall be entered into the JPAS by the appropriate CAF.

C3.4.4.5.5. The administrative action procedures in Chapter 9 do not apply to LAA determinations.

#### C3.4.4.6. Record

C3.4.4.6.1. The LAA granting authority shall ensure that a record is created upon issuance and is maintained for five years from the date the LAA ceases. The record shall include the following:

C3.4.4.6.1.1. Identity of the person granted the LAA, to include the full name, date and place of birth, current citizenship(s), any Social Security Number (SSN), and any national identifying number issued by the individual's country or countries of citizenship;

C3.4.4.6.1.2. Person's status as a non-U.S. citizen; and the date and place such status was granted;

C3.4.4.6.1.3. Classification level of the LAA; i.e., SECRET or CONFIDENTIAL;

C3.4.4.6.1.4. Date and type of most recent background investigation or PR and the investigating agency;

C3.4.4.6.1.5. Conduct of a polygraph examination. If so, the date and administering agency for the most recent examination.

C3.4.4.6.1.6. Nature and identity of the classified program materials to which access is authorized and the precise duties performed.

C3.4.4.6.1.7. The compelling reasons for granting access to the information.

C3.4.4.6.2. All LAA SSBI and PRs shall be conducted under the auspices of DSS and shall comply with the requirements of Appendix 1. The DSS 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 DSS for review and entry into the DCII, and then returned 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 DSS for assignment of a case control number and initiation of such other checks as needed.

C3.4.4.6.3. The Combatant Commands shall report LAAs they issue to the applicable DoD Component CAF for entry into the JPAS. The Combatant Commands shall ensure that all investigative paperwork for the initiation of the SSBI or PR is submitted to the DSS through the designated single-approval authority responsible for adjudication and issuance of the LAA.

C3.4.4.6.4. All LAA nominees must agree to undergo a polygraph examination at any time during the period the LAA is in effect, provided there is no host-country legal prohibition.

C3.4.4.7. All LAAs shall be reviewed annually by the issuing component to determine if continued access is in compliance with DoD policy. DoD Components shall maintain a record of all LAAs in effect, to include the data required in subparagraph C3.4.4.6. and furnish such documentation to DASD(S&IO) upon request. A summary report by level of LAA and country location shall be furnished to DASD(S&IO) within 60 days after the end of each fiscal year.

#### C3.4.5. Access by Consultants to DoD Components

C3.4.5.1. A consultant who is hired by a DoD Component and will only require access to classified information at the Component's activity or in connection with authorized visits is considered an employee of the DoD Component and does not fall under the National Industrial Security Program (NISP). The consultant will be issued a clearance in accordance with Chapter 8.

C3.4.5.2. Investigations required to support the consultant's security clearance shall be conducted by the investigative provider and adjudicated by the DoD Component CAF. The unfavorable administrative action procedures provided in Chapter 9 apply.

C3.4.5.3. When compelling reasons exist, non-U.S. citizens functioning as consultants to DoD Components as defined by subparagraph C3.4.5.1. may be considered for LAA in accordance with subparagraph C3.4.4.

#### C3.4.6. Restrictions on Issuance of Personnel Security Clearances

C3.4.6.1. Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements.

C3.4.6.2. Personnel security clearances shall normally not be issued:

C3.4.6.2.1. To persons in nonsensitive positions.

C3.4.6.2.2. To persons whose regular duties do not require access to classified information.

C3.4.6.2.3. For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

C3.4.6.2.4. 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.

C3.4.6.2.5. To persons working in shipyards whose duties do not require access to classified information.

C3.4.6.2.6. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

C3.4.6.2.7. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

C3.4.6.2.8. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

C3.4.6.2.9. To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

C3.4.6.2.10. To perimeter security personnel who have no access to classified information.

C3.4.6.2.11. To drivers and chauffeurs.

C3.4.7. Dual Citizenship. Persons claiming both U.S. and foreign citizenship shall be processed under section C3.4. and adjudicated in accordance with the "Foreign Preference" standard in Appendix 5.

C3.4.8. 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 prevent timely access to the information. In such situations, and only for compelling reasons in furtherance of the DoD mission, an active duty flag or general officer or civilian equivalent, 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 that would permit the routine processing of an individual for the higher level clearance. Procedures and conditions for effecting one-time access to the next higher classification level are as follows:

C3.4.8.1. Conditions for temporary granting of higher level access:

C3.4.8.1.1. It is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

C3.4.8.1.2. Will not exceed 180 days; and

C3.4.8.1.3. Is limited to specific, identifiable information that is made the subject of a written record.

C3.4.8.2. Procedures for temporary granting of higher level access:

C3.4.8.2.1. Authorization for such one-time access shall be granted by a flag or general officer, a general court martial convening authority, or ES-1 or higher, after coordination with appropriate security officials.

C3.4.8.2.2. 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 recipient's current clearance.

C3.4.8.2.3. Such access shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

C3.4.8.2.4. 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-time employees.

C3.4.8.2.5. Local employee personnel and security records of the employee concerned shall be reviewed with favorable results.

C3.4.8.2.6. 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: (1) recording the higher-level information actually revealed, (2) the date(s) such access is afforded, and (3) the daily retrieval of the material accessed.

C3.4.8.2.7. Access at the next higher level for Communications Security (COMSEC), SCI, North Atlantic Treaty Organization (NATO), or foreign government information is not authorized.

C3.4.8.2.8. The authorizing authority shall maintain a record for two years from the date access is granted, containing the following data with respect to each access approved:

C3.4.8.2.8.1. The name and SSN of the employee afforded higher level access.

C3.4.8.2.8.2. The level of access authorized.

C3.4.8.2.8.3. 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.

C3.4.8.2.8.4. 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.

C3.4.8.2.8.5. A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

C3.4.8.2.8.6. The approving authority's signature certifying subparagraphs C3.4.8.2.8.1. through C3.4.8.2.8.5.

C3.4.8.2.8.7. Copies of any pertinent briefings and/or debriefings administered to the employee.

#### C3.4.9. Access by Retired Flag and/or General Officers or Civilian Equivalent

C3.4.9.1. Upon determination by an active duty flag or general officer or civilian equivalent that there are compelling reasons, in furtherance of the DoD mission, to grant a retired flag or general officer or civilian equivalent access to classified information in connection with a specific DoD program or mission, for a period not greater than 180 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 and within 24 months of retirement.

C3.4.9.2. The flag or general officer or civilian equivalent approving the access to classified information shall provide the appropriate DoD Component CAF a written record to be incorporated into JPAS detailing:

C3.4.9.2.1. Full identifying data pertaining to the cleared subject;

C3.4.9.2.2. The classification of the information to which access will be authorized.

C3.4.9.3. Access may be granted only after the compelling reason and the specific aspect of the DoD mission that is served by granting 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. POSITIONS NOT REQUIRING ACCESS TO CLASSIFIED INFORMATION

#### C3.5.1. Trustworthiness Determinations.

C3.5.1.1. When there is no bona fide requirement for access to classified information in the performance of assigned duties, a security clearance should not be requested. However, a requirement to conduct an investigation may still exist depending upon the national security significance of the area, material, or sensitivity of the information involved. The purpose of these investigations is to provide some assurance that personnel in these positions are trustworthy. This investigative requirement will impact primarily contractor personnel. Military and civilian personnel undergo an investigation for entry into government service.

C3.5.1.2. A NAC is the baseline investigation for these positions unless otherwise specified. Entry investigations for military (NACLC) and civilian (NACI) personnel satisfy the baseline investigative requirement. OPM will conduct all trustworthiness investigations for DoD. DoD Components shall include guidance indicating the investigation is for a trustworthiness determination and the specific duty, function or situation that requires it. Investigative requests are to be submitted on an SF86 and forwarded to OPM per Appendix 2.

C3.5.1.3. Completed investigations are to be returned to OPM (SOI: OM25) for a trustworthiness determination. Adverse cases will be sent to the Defense Office of Hearings and Appeals (DOHA) for final action. The submitting entity will be notified in writing regarding the results of the OPM/DOHA decision. The adjudicative guidelines in Appendix 5 and the procedures in Chapter 9 will serve as the basis for most decisions. In certain cases, status as a non-U.S. citizen is not an automatic disqualifier. For contractor personnel, trustworthiness determinations are outside the provisions of the NISP.

C3.5.1.4. DoD Components are to issue guidance to their own personnel and to contractors under contract to them to ensure investigative requests to OPM contain the appropriate billing code for the DoD Component.

C3.5.1.5. Personnel in these positions shall be subject to a random aperiodic reinvestigation under the forthcoming Automated Continuing Evaluation System (estimate: June 2003).

C3.5.2. Military Installations. Per DoD Directive 5200.8 (reference (w)) military Commanders can issue orders and regulations for the protection of property or places under their command. There are certain categories of positions or duties that if performed by untrustworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security.

### C3.5.3. Red Cross and/or United Service Organizations Personnel

C3.5.3.1. Red Cross and United Service Organization (USO) employees shall be accepted for assignment or for continued assignment with Military Services overseas provided such acceptance is consistent with the national interest. The security acceptability of an employee for assignment or continued assignment with the Military Services overseas shall be determined in accordance with DoD Directive 5220.6 (reference (d)). In the event the employee will require access to classified information, he and she will be processed for the appropriate level of security clearance in accordance with the requirements of this Regulation.

#### C3.5.3.2. Procedures

C3.5.3.2.1. U. S. citizen and non-U.S. citizen employees shall have been the subjects of a favorable NACLIC before being nominated for assignment with the Military Services overseas.

C3.5.3.2.2. The above does not apply to U. S. citizens or non-U.S. citizens who are available locally at overseas stations for temporary or part-time employment with the Red Cross or USO. The Military Department concerned shall determine policy and procedures governing investigation and security acceptability of locally hired employees.

C3.5.3.2.3. A completed SF 86 shall be forwarded to the DSS for the initiation of the NACLIC per Appendix 2.

C3.5.3.2.4. The results of the investigation shall be forwarded to DSS for a security acceptability determination of the employee. DSS shall provide the Red Cross or USO with a statement on all favorable determinations. Whenever DSS is unable to make a favorable security acceptability determination, the case shall be referred for further action in accordance with DoD Directive 5220.6 (reference (d)).

C3.5.3.2.5. Whenever information of an adverse nature is received indicating that an employee's assignment or continued assignment with the Military Services overseas may not be consistent with the national interest, the information shall be forwarded to DSS for appropriate review.

C3.5.3.2.5.1. DSS may initiate an investigation or expand an ongoing investigation to resolve the issue(s).

C3.5.3.2.5.2. No further action will be required of DSS if the adjudication of the alleged adverse information and/or subsequent investigative reports is favorable.

C3.5.3.2.5.3. Any unfavorable adjudication shall be processed as outlined in subparagraph C3.5.3.2.4.

C3.5.3.3. DSS shall serve as the contact for the Red Cross and USO in all matters pertaining to the procedures stated above.

C3.5.4. Non-U.S. citizen Employees Overseas. A non-U.S. citizen employed by DoD Components overseas, whose duties do not require access to classified information, shall be the subject of at least the following record checks, initiated by the appropriate Military Department investigative organization prior to employment. These checks and any additional investigation must be consistent with the policy and procedures governing locally hired employees under Status of Forces Agreements. DoD Components assume responsibility for permitting access to DoD systems, information, material, and areas when an investigation conducted by the host country does not meet the investigative standards of this Regulation.

C3.5.4.1. 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

C3.5.4.2. DCII/JPAS

C3.5.4.3. FBI (where information exists indicating residence by the non-U.S. citizen in the United States for one year or more since age 18)

C3.5.4.4. CIA as appropriate

C3.5.5. Personnel Occupying Information Technology or Related Positions. DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified Information Technology Systems (IT) or in IT related positions are subject to the policy and investigative requirements contained in Appendix 6. Those personnel who require access to classified information are subject to the appropriate investigative scope in section C3.4.

## C3.6. REINVESTIGATION

C3.6.1. 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 Appendix 1, to meet overall security requirements. Reinvestigation, generally, is authorized only as follows:

C3.6.1.1. To prove or disprove an allegation relating to the criteria set forth in Chapter 2 with respect to an individual holding a security clearance, occupancy of a sensitive position or assigned to a position that requires a trustworthiness determination.

C3.6.1.2. To meet the periodic reinvestigation requirements of this Regulation.

C3.6.1.3. Upon individual request, to assess the current eligibility of persons 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 exist.

C3.6.1.4. Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the security standard criteria outlined Chapter 2 that could impact on an individual's security status, an 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 subparagraph C9.2.2.

### C3.7. AUTHORITY TO WAIVE INVESTIGATIVE REQUIREMENTS

Only Heads of DoD Components or designee are empowered to grant an exception from 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. A minor investigative element that has not been met should not preclude favorable adjudication, nor should this require an exception when all other information developed on an individual during the investigation is favorable. For SCI access, only the Director of Central Intelligence (DCI) or cognizant SOIC may authorize access to SCI prior to completion of the investigation. Only the DCI can authorize access to SCI without benefit of an investigation.

## C4. CHAPTER 4

### ASSOCIATED PROGRAMS

#### C4.1. GENERAL

All of the programs listed in this Chapter require a PSI in addition to meeting other requirements before initial or continued access or admittance to the program is granted. Due to tradition, a listing of these programs is provided for ease of reference. In all instances the applicable directive, instruction or publication should be used as the definitive policy source for that program, not this Regulation.

#### C4.2. SENSITIVE COMPARTMENTED INFORMATION (SCI)

C4.2.1. Personnel security requirements for access to SCI are set forth in DCID 6/4 (reference (k)). Access to SCI is a security determination made under the cognizance of a SOIC.

C4.2.2. An individual and all immediate family members must be citizens of the United States and be free from duress by foreign or criminal entities. The cognizant SOIC may grant exception to the above criteria regarding family members. Only the DCI may grant exception to the citizenship requirement for the individual

C4.2.3. A Top Secret security clearance is not a prerequisite for access to SCI. A favorable determination of eligibility for access to SCI shall constitute a favorable determination of eligibility for access to Top Secret and below.

C4.2.4. An SSBI is the investigative basis for SCI access. An existing SSBI conducted within the past five years may serve as a basis for granting SCI access, provided that the investigation was conducted and adjudicated for SCI access in accordance with DCID 6/4 (reference (k)) and that the break in SCI access was less than 24 months. The subject shall submit one copy of an updated SF 86 covering the period since the completion of the last SSBI and certify any substantive changes that may have occurred. Investigation shall be conducted as required to update the investigation and/or to resolve potentially disqualifying information. The cognizant SOIC is authorized to grant exception to the requirement for a current investigation prior to granting access to SCI. Only the DCI is authorized to grant access to SCI without benefit of an investigation.

C4.2.5. Access to SCI may be granted only by the DCI, a SOIC or designated Determination Authority and only to those individuals who meet stringent personnel security standards set for in DCID 6/4 (reference (k)) and have a demonstrated need to know. Members of Congress and Federal judges and, under certain circumstances, state governors are exempted from this provision; however, the conditions of access to SCI must be approved by the DCI or cognizant SOIC.

C4.2.6. In accordance with Annex F, DCID 6/4 (reference (k)) a favorable SCI access determination based on investigation and adjudication in accordance with DCID 6/4 (reference

(k)) and which is without exception for access, shall be mutually and reciprocally accepted by all DoD SOICs. SCI eligibility accesses having exceptions are not transferable, unless the gaining SOIC accepts such exception upon completion of a risk management review. All DoD SOICs for a minimum of one year shall enforce unfavorable eligibility determinations.

C4.2.7. The denial or revocation of SCI access shall be accomplished by the DCI, SOIC or designated Determination Authority when an individual fails to satisfy the stringent personnel security criteria set forth in DCID 6/4 (reference (k)). Individuals shall have the right to appeal such denial or revocation determinations in accordance with the provisions of Annex D, DCID 6/4 (reference (k)). In those instances wherein access to SCI is denied or revoked, immediate action shall be taken to notify appropriate collateral clearance authorities so that relevant information can be assessed against collateral clearance criteria.

### C4.3. SPECIAL ACCESS PROGRAMS (SAPs)

C4.3.1. A SAP is a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level under E.O. 12958 (reference (a)) and prior Executive Orders. SAP policy and procedures are contained in DoD O-5205.7 (reference (x)), DoD Instruction S-5205.11 (reference (y)), and Chapter 8, DoD 5200.1-R (reference (u)).

#### C4.3.2. Program Requirements and Procedures.

C4.3.2.1. Generally, all candidates for SAP access must be U.S. citizens. As a minimum, access to SAP information must be based on a final Secret clearance current within five years. If a person, in a continuous clearance status, has an investigation outside the five year scope, the Program Security Officer (PSO) or other access granting authority may grant a waiver for the investigative basis and authorize access. Access waivers are based on (a) completion and submission of the investigative forms; (b) a review to ensure no identifiable significant derogatory or security concerns exist; and (c) a favorable DCII check. Subsequent to the decision to access the individual to a DoD controlled SAP; the person will be immediately processed for a PR.

C4.3.2.2. There are two sensitivity levels for SAP access. Baseline access requires a Secret or Top Secret security clearance based on an investigation not more than five years old. Enhanced requirements include the baseline requirements plus a uniform SAP enhancement package and updated personnel security information. Some SAPs operate jointly with the Intelligence Community and require access to SCI. Persons with access to joint SAP/SCI programs must meet both enhanced SAP (or if appropriate waived SAP) and SCI requirements.

C4.3.2.3. Eligibility for SAP access will be determined utilizing, as a basis, the guidelines reflected in this Regulation, DCID 6/4 (reference (k)), or other appropriate adjudication guidelines which have been authorized for use within the Department by the DoD Special Access Program Oversight Committee (SAPOC). The number of persons granted access to a DoD SAP must be strictly limited to the minimum necessary for execution and management oversight of the program. The cognizant OSD level SAP central office and the Director of

Security, OASD(C3I) must approve upgrades to investigative standards and unique adjudicative criteria.

C4.3.2.4. SAP access eligibility determinations shall be mutually and reciprocally accepted by all DoD Components. However, reciprocity of SAP access eligibility is not required when SAP access was granted based on an exception to the access criteria or standard or there is a subsequent security concern. An examination of the exception resulting from adjudication of the adverse information or security concern may be imposed prior to granting SAP access.

C4.3.2.5. Acknowledged SAP accesses may be placed into appropriate central databases where operations security factors is not a consideration. SAP access determination information should be entered into the JPAS within 24 hours. Because of the extreme sensitivity and compartmentation, Unacknowledged or Waived SAP accesses (i.e., subsection 119e, Title 10, USC (reference (z))), may only be recorded in compartmented data bases (as soon as practicable) which are protected at or above the program security protection standard. The investigative basis for determining the accesses may be recorded in the JPAS or other indexes only if the record does not provide insight into the classified nature of the individual access. In those instances where individual investigative records, for SAP security reasons, cannot be placed into the JPAS, the DoD Component must maintain its own compartmented data base or work with the Special Access Program Coordination Office (SAPCO) to record the information within the SAPCO compartmented security information network.

#### C4.3.3. Access Suspension and Revocation.

C4.3.3.1. The suspension or revocation of SAP access, as well as the SAP appeal process, will be accomplished in accordance with this Regulation and/or the appeal procedures outlined in DCID 6/4 (reference (k)). In those instances where revocations or suspensions are for cause, immediate action must be taken to notify appropriate collateral clearance authorities so that the security significance of the situation can be assessed. When security measures cannot otherwise be accommodated, notifications may be processed through the Director, Security, OASD (C3I).

C4.3.3.2. Suspension or revocation (i.e., withdrawal) of SAP access will be provided in writing and follow the general concepts outlined in Annex B of DCID 6/4 (reference (k)). Authority to grant, deny, or revoke access to SAP is a function of the DoD Component level or OSD level SAP Central Office or their designated representative(s). The authority for making SAP access determinations may not necessarily be the same official making security clearance determinations. Procedures for unfavorable decisions regarding access to DoD SAPs may differ from the procedures in this Regulation and as approved by the Secretary or Deputy Secretary of Defense. SAP access determinations are an adjudicative function relating to a person's suitability for such access.

C4.3.3.3. Denial, revocation, or limitation of a candidate's SAP access is an access decision only and may not be the basis for further unfavorable administrative actions. It cannot--and does not--render an individual ineligible for access to other classified information based

solely on denial of SAP access. It does not reflect on any other aspect of the candidate's loyalty, trustworthiness or reliability.

C4.4. SINGLE INTEGRATED OPERATIONAL PLAN-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI). JSCM 36-76 (reference (aa)) outlines policies and procedures for access to SIOP-ESI. The applicant and spouse must be U.S. citizens. The investigative requirement for access to SIOP-ESI is an SSBI. Any unfavorable actions pertaining to contractor employees are governed by DoD Directive 5220.6 (reference (d)).

C4.5. RESTRICTED DATA AND CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI). DoD Directive 5210.2 (reference (bb)) prescribes the policies and procedures governing access to and dissemination of Restricted Data and CNWDI.

C4.6. PRESIDENTIAL SUPPORT ACTIVITIES. DoD Directive 5210.55 (reference (cc)) 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.

C4.7. NUCLEAR WEAPON PERSONNEL RELIABILITY PROGRAM (PRP). DoD Directive 5210.42 (reference (dd)) sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and critical components.

C4.7.1. Explosive Ordnance Disposal (EOD). Although such personnel normally only require a Secret clearance, an SSBI is initially required due to training and assignment involving nuclear weapons. Additionally, each person occupying an EOD position shall undergo a Secret PR on a five year recurring basis. Personnel with current access to Top Secret information are subject to an SSBI-PR every five years.

C4.8. CUSTOMS INSPECTORS. DoD employees appointed as customs inspectors, under waivers approved in accordance with DoD 5030.49-R (reference (ee)), shall have a favorably adjudicated NACLIC or NACI completed within the past five years unless there has been a break in DoD employment greater than 24 months in which case a current investigation is required.

C4.9. 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 NACLIC or NACI completed within the last five years prior to assignment in accordance with DoD Directive 5210.65 (reference (ff)).

C4.10. ACCESS TO NATO CLASSIFIED INFORMATION

C4.10.1. Personnel assigned to a NATO staff position requiring access to NATO COSMIC (Top Secret), Secret or Confidential information shall have been the subject of the requisite investigation current within five years prior to the assignment, in accordance with USSAN Instruction 1-69 (reference (gg)).

C4.10.2. U.S. military personnel shall be permitted temporary access to COSMIC information based on a final U.S. Secret clearance and issuance of an interim Top Secret clearance, pending completion of an SSBI and issuance of a final Top Secret clearance. The temporary access eligibility will be valid until completion of the investigation and adjudication of the final clearance. However, the agency granting the access will rescind it if unfavorable information is identified in the course of the investigation.

C4.10.3. A person may be assigned to a NATO Secret or Confidential billet based on a U.S. Secret clearance with a request for PR submitted to the investigative provider.

C4.10.4. Personnel not assigned to a NATO staff position, but requiring access to NATO COSMIC, Secret or Confidential information in the normal course of their duties, must possess the equivalent U.S. security clearance based upon the appropriate personnel security investigation.

C4.10.5. Interim procedures as outlined in C4.10.2. apply to personnel not assigned to a NATO staff position, but requiring access to NATO COSMIC, Secret or Confidential information.

C4.10.6. When access to NATO classified information by a national of a NATO member nation is proposed, a NATO Security Clearance Certificate shall be obtained from the person's National Security Authority prior to access being approved. If access is required by a person who is not a national of a NATO member nation, approval for release of the NATO classified information must be obtained from the appropriate NATO committee. (See USSAN Instruction 1-69 (reference (gg)) for further details.)

C4.10.7. Interim access to NATO classified information based on a pending LAA is not authorized. Requests for access to NATO classified information for a national of a non-NATO nation based on an LAA shall be referred to the USSAN, with complete justification. The requests shall include the information required in subparagraphs C3.4.4.4.6. and C3.4.4.6. Upon approval of the LAA, the individual will be given a briefing by the requesting agency's cognizant security office regarding responsibilities for protecting NATO classified information. A NATO briefing certificate prescribed by USSAN Instruction 1-69 (reference (gg)) shall be executed.

C4.11. ARMS, AMMUNITION AND EXPLOSIVES (AA&E). DoD 5100.76-M (reference (hh)) requires personnel assigned custody, maintenance, disposal, or security responsibilities for AA&E on military installations as well as those operating a vehicle or providing security to a vehicle in transporting AA&E shall be the subject of a favorably completed NACLIC or NACI.

C4.12. CONTRACT LINGUISTS. DoD Components have found it necessary to contract for linguists to supplement internal language capabilities to support military deployments and operations. These linguists frequently have cultural, familial, financial or political ties to the theater in which they deploy. These ties, coupled with a potentially hostile deployment environment, raise force protection concerns and the need for consistency in the screening, vetting and hiring of contract linguists throughout the Department.

C4.12.1. While contract responsibility for hiring linguists rests with the DoD Components, recent events indicate a standard procedure is needed to ensure uniformity in the processing of contract linguists, address disparate processes, and lessen security risks to other DoD Components in theater. These procedures shall be included in Component directives as the governing and source guidance.

C4.12.2. The contract, at a minimum, must require pre-deployment screening of all contract linguists and if required a security clearance determination by the appropriate CAF. A personnel security investigation will be conducted on all individuals employed as contract linguists. DoD Components will establish procedures for the hiring and vetting of contract linguists within the U.S. as well as overseas.

C4.12.3. The terms of the contract should address government screening, investigation, and disqualification of a linguist. The screening is to occur after a conditional offer of employment by the contractor and prior to deployment or utilization of the linguist. The screening process may include use of a polygraph, particularly if SCI access is required and a check of appropriate databases. The contract must specify that the screening will be done prior to initiation of the investigation and that the individual must successfully pass the screening procedure before the investigation is initiated. Additionally, the employing company must screen the applicants to ensure they meet established employment criteria, including U.S. citizenship verification when required. Non-U.S. citizens are not eligible for assignment in positions with access to classified information.

C4.12.4. DoD Component procedures should include command responsibilities for contract specifications, screening procedures, security clearance determinations, initiation of the investigation, maintenance and storage of screening documentation, annotation of JPAS, and briefing and debriefing procedures. All investigations for contract linguists hired in the U.S. will be conducted by DSS. DoD Components will coordinate conduct of the investigation for contract linguists hired overseas with DSS.

C4.12.5. Investigations for contract linguists are designated a priority. DoD Components are to coordinate with DSS to determine if additional procedures or annotating of investigative requests for contract linguists are needed.

## C5. CHAPTER 5

### RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

#### C5.1. 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 personnel have been previously cleared or investigated by the U.S. Government. Any previously granted security clearance or access, 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 unless subsequent derogatory information is known to exist. Previously conducted investigations and previously rendered personnel security determinations shall be accepted within the Department in accordance with the policy in section C5.4.

#### C5.2. 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 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 section C2.3 of Chapter 2 and subparagraph C5.3.2.

#### C5.3. PRIOR PERSONNEL SECURITY DETERMINATIONS MADE BY DoD AUTHORITIES

C5.3.1. Adjudicative determinations concerning an individual's eligibility for access to classified information or assignment to sensitive duties made by designated DoD authorities shall be mutually and reciprocally accepted by all DoD Components. An investigation shall not be requested, unless there has been a break in the individual's military service and/or employment greater than 24 months or unless derogatory information that occurred subsequent to the last security determination is known. A check of JPAS or other appropriate databases should be conducted to accomplish this task.

C5.3.2. Whenever a valid DoD security clearance or access eligibility is on record, Components shall not request investigative providers or other DoD investigative organizations to forward prior investigative files for review unless:

C5.3.2.1. Significant derogatory information or investigation completed subsequent to the date of last clearance and/or access authorization, is known to the requester; or

C5.3.2.2. The person concerned is being considered for a higher level clearance or access (e.g., SECRET, TOP SECRET or SCI) or the person does not have an access authorization and is being considered for one; or

C5.3.2.3. The most recent clearance or access authorization of the person concerned was based on an exception.

C5.3.3. The investigative provider shall obtain all non-DoD investigative files by the most expeditious means possible.

C5.3.4. Whenever a civilian or military member transfers from one DoD activity to another, the losing organization's security office shall advise the gaining organization of any 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.

#### C5.4. INVESTIGATIONS CONDUCTED AND CLEARANCES GRANTED BY OTHER AGENCIES OF THE FEDERAL GOVERNMENT

C5.4.1. A prior investigation or personnel security determination by another Agency of the Federal Government that meets the investigative scope and standards of this Regulation shall be accepted if there is no break in service longer than 24 months and inquiry 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.

C5.4.2. To be consistent with the philosophy of reciprocity and to ensure equitable due process, DoD Components shall ensure the timely investigation and adjudication of civilian employees and military personnel as required. DoD Components will provide the personnel security determination information to other DoD organizations via JPAS or other agencies of the Federal Government to which the individual is assigned or detailed.

C5.4.3. DoD policy on reciprocal acceptance of clearances with the Nuclear Regulatory Commission and the Department of Energy is set forth in DoD Directive 5210.2 (reference (bb)).

## C6. CHAPTER 6

### REQUESTING PERSONNEL SECURITY INVESTIGATIONS

#### C6.1. GENERAL

Requests for PSIs shall be limited to those required to accomplish the DoD mission. Only the authorities designated herein shall submit such requests. 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.

#### C6.2. AUTHORIZED REQUESTERS

Requests for personnel security investigations shall be accepted only from those designated below:

##### C6.2.1. Military Departments

###### C6.2.1.1. Army

C6.2.1.1.1. Central Adjudication Facility

C6.2.1.1.2. All activity commanders

C6.2.1.1.3. Chiefs of recruiting stations

###### C6.2.1.2. Navy (including Marine Corps)

C6.2.1.2.1. Central Adjudication Facility

C6.2.1.2.2. Commanders and commanding officers of organizations listed on the Standard Navy Distribution List

C6.2.1.2.3. Chiefs of recruiting stations

###### C6.2.1.3. Air Force

C6.2.1.3.1. Central Adjudication Facility

C6.2.1.3.2. Director, Intelligence, Surveillance, and Reconnaissance

C6.2.1.3.3. All activity commanders

C6.2.1.3.4. Chiefs of recruiting stations

C6.2.2. Defense Agencies. Directors of Security and activity commanders

C6.2.3. Chairman of the Joint Chiefs of Staff. Chief, Security Division

C6.2.4. Office of the Secretary of Defense. Director for Personnel and Security, Washington Headquarters Services, and Central Adjudication Facility

C6.2.5. Commanders of Combatant Commands or their designees

C6.2.6. Defense Office of Hearings and Appeals

C6.2.7. Such other requesters approved by the DASD(S&IO).

### C6.3. REQUEST PROCEDURES

To insure efficient and effective completion of required investigations, all requests for PSIs shall be prepared and forwarded in accordance with Appendix 2 and the investigative jurisdictional policies set forth in section C2.4.

### C6.4. PRIORITY REQUESTS

To ensure that PSIs are conducted in an orderly and efficient manner, requests for priority of individual investigations or categories of investigations shall be kept to a minimum. Appendix 9 establishes the priorities for DoD investigations. DASD(S&IO) in coordination with requesters, is to review and update these investigative priorities or its successor every two years.

### C6.5. PERSONAL DATA PROVIDED BY THE SUBJECT OF THE INVESTIGATION

C6.5.1. 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 requires that, to the greatest extent practicable, personal information be obtained directly from the subject when the information may result in adverse determinations affecting the subject's rights, benefits, and privileges under Federal programs.

C6.5.2. Accordingly, it is incumbent upon the subject of each PSI to provide the personal information required by this Regulation. At a minimum, the subject 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.

C6.5.3. 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 person's security clearance or assignment to sensitive duties utilizing the procedures of subparagraph C9.2.2 or further administrative processing of the investigative request.

## C7. CHAPTER 7

### ADJUDICATION

#### C7.1. GENERAL

C7.1.1. The principal objective of the DoD personnel security adjudicative function is to assure selection of persons for clearance or placement in sensitive positions. The adjudication process involves an assessment of the probability of future behavior that 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.

C7.1.2. 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 which could, if abused, have unacceptable consequences for the national security.

C7.1.3. While equity demands optimal uniformity in evaluating individual cases, ensuring 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.

#### C7.2. CENTRAL ADJUDICATION

C7.2.1. To ensure uniform application of the criteria and guidelines in this Regulation and to ensure that DoD personnel security determinations are effected consistent with existing statutes and Executive Orders, only the authorities listed in Appendix 3 are authorized to make such decisions. The function of such authorities shall be limited to evaluating personnel security investigations and making personnel security determinations. The chief of each CAF 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 experienced personnel security specialists specifically designated by the head of the Component concerned, or designee. No clearance or access eligibility determination may be made in the absence of such review.

C7.2.2. 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, sufficient levels of

review as well as management oversight shall be required for all clearance and/or access determinations, especially those containing adverse information.

C7.2.2.1. SSBI and SSBI/PRs that are not completely favorable shall undergo at least two levels of review by adjudication 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, the Statement of Reasons (SOR) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS-14 or the military rank of O-5. A final notification of denial or revocation of clearance or access must be approved and signed at the civilian grade of GS-15 or the military rank of O-6.

C7.2.2.2. An adjudicative official in grades GS-7/9 or O-3 must review investigations of lesser scope that are not completely favorable. When an unfavorable administrative action is contemplated, an adjudicative official in grade GS-12/13 or O-4/5 must sign the SOR. A final notification of denial or revocation of clearance or access must be approved and signed at the civilian grade of GS-14/15 or the military rank of O-5 or above.

C7.2.3. In order to meet increasing mission requirements, CAFs have found it necessary to augment their staffs. While final adjudicative determinations are an inherently governmental function, DoD Components may contract for adjudicative support services. These services may include screening cases for investigative compliance, creating a written record of issue(s) in the case and making adjudicative recommendations. Government personnel shall make all final adjudicative determinations. Contract adjudicative support personnel must meet the same clearance and investigative requirements as well as job expertise as government personnel. Contract adjudicative personnel shall be subject to continuous review of CAF personnel and shall work only at a CAF. DoD Components shall include these requirements in the contract.

### C7.3. EVALUATION OF PERSONNEL SECURITY INFORMATION

C7.3.1. The criteria and adjudicative policy to be used in applying the principles at section C7.1. are set forth in section C2.2. and Appendix 5 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:

C7.3.1.1. The nature, extent and seriousness of the conduct;

C7.3.1.2. The circumstances surrounding the conduct, to include knowledgeable participation;

C7.3.1.3. The frequency and recency of the conduct;

C7.3.1.4. The person's age and maturity at the time of the conduct;

C7.3.1.5. The voluntariness of participation;

C7.3.1.6. The presence or absence of rehabilitation and other pertinent behavioral changes;

C7.3.1.7. The motivation for the conduct;

C7.3.1.8. The potential for pressure, coercion, exploitation or duress; and

C7.3.1.9. The likelihood of continuation or recurrence.

C7.3.2. 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 5. Adjudication policy for access to SCI is contained in DCID 6/4 (reference (k)). Adjudicators shall also make use of the guidance contained in the Adjudicators Desktop Reference (ADR).

#### C7.4. ADJUDICATIVE RECORD

C7.4.1. Each adjudicative determination, whether favorable or unfavorable, shall be entered into JPAS on a daily basis.

C7.4.2. 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 derogatory information of the type set forth in Section C2.2. and Appendix 5 of this Regulation, shall be maintained in written or automated form in JPAS and is subject to the provisions of DoD Regulations 5400.7-R (reference (ii)) and 5400.11-R (reference (jj)). This information shall be maintained for a minimum of five years from the date of determination or for as long as the individual is affiliated with DoD, whichever is longer.

## C8. CHAPTER 8

### ISSUING CLEARANCES AND GRANTING ACCESS

#### C8.1. GENERAL

C8.1.1. The issuance of a personnel security clearance or determination of SCI or SAP access eligibility (as well as determining that a person is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from the granting of access to classified information. Clearance or access eligibility determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance.

C8.1.2. Access determinations are made solely on the basis of the person'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 provision of subparagraph C9.2.2.

C8.1.3. Only the authorities designated in Appendix 3 are authorized to grant, deny or revoke personnel security clearances, or SCI access eligibility determinations. Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to the person's ability or intent to protect classified information, provided that the procedures set forth in subparagraph C9.1.2. are complied with.

C8.1.4. All commanders and heads of DoD organizations have the responsibility for determining those positions 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.

#### C8.2. ISSUING CLEARANCE

C8.2.1. Authorities designated in Appendix 3 shall record the issuance, denial, or revocation of a personnel security clearance or SCI access eligibility in JPAS. A record of the clearance issued shall also be recorded in the subject's personnel and/or security file or official personnel folder, as appropriate.

C8.2.2. A personnel security clearance or eligibility determination remains valid until (a) the person is separated from the Armed Forces; (b) separated from DoD civilian employment; (c) has no further official relationship with the DoD; (d) official action has been taken to deny, revoke or suspend the clearance or access; or (e) regular access to the level of classified information for which the person holds a clearance is no longer necessary in the normal course of his and her duties. In the latter instance, access-granting officials will take appropriate action to terminate, administratively withdraw or downgrade access as appropriate and record in JPAS when such action is taken. If a person resumes the original status of a. through c, and e., above, no single break in his or her relationship with the DoD 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/access may be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

C8.2.3. Personnel security clearances and eligibility determinations 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 of Army, Navy, and Air Force personnel 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 to the employing activity. 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 person's parent Component. Whenever the employing DoD Component issues an interim clearance to an individual from another Component, notice of the action shall be provided to the parent Component via JPAS.

C8.2.4. 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 Chiefs of Staff, the completed investigation will be returned to the appropriate Military Department CAF 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 via JPAS. For military personnel assigned to 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, via entry in JPAS.

C8.2.5. When an SSBI (or PR) for access to SCI is initiated on a contractor employee, the completed investigation will be returned to the appropriate CAF with SCI cognizance. Following a favorable SCI eligibility determination, the CAF will notify DSS of the outcome via JPAS. If the SCI eligibility is denied or revoked, the CAF will complete all due process and appeal procedures. The case and all relevant additional documentation will then be sent to DSS for appropriate action, to include referral to DOHA for possible action under DoD Directive 5220.6 (reference (d)).

C8.2.6. Interim clearances shall be recorded in JPAS by the cognizant CAF in the same manner as a final clearance.

### C8.3. GRANTING ACCESS

C8.3.1. Access to classified information shall be granted to persons whose official duties require such access and who have the appropriate personnel security clearance. Such determinations (other than for SCI or SAPs) are not an adjudicative function relating to a person's suitability for such access. Rather they are decisions made by the commander that access is officially required.

C8.3.2. In the absence of derogatory information concerning the person 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 clearances, as the basis for granting access, when access is required, without requesting additional investigation or investigative files.

C8.3.3. The access level of cleared personnel will be entered into JPAS along with clearance eligibility.

#### C8.4. ADMINISTRATIVE WITHDRAWAL

As set forth in section C8.2. the personnel security clearance or access eligibility must be administratively downgraded or withdrawn when the events described therein occur. When access to a prescribed level of classified information is no longer required in the normal course of a person's duties, the previously authorized access eligibility level must be administratively downgraded or withdrawn, as appropriate and recorded in JPAS.

## C9. CHAPTER 9

### UNFAVORABLE ADMINISTRATIVE ACTIONS

#### C9.1. REQUIREMENTS

C9.1.1. General. For purpose of this Regulation, an unfavorable administrative action includes any negative action that is taken as a result of a personnel security determination. This chapter is intended only to provide guidance for the internal operation of the Department of Defense. It 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 (MSPB).

#### C9.1.2. Referral for Action

C9.1.2.1. Whenever derogatory information is developed or otherwise becomes available to any DoD element, it shall be referred to the commander or the security officer of the organization to which the person is assigned for duty. For contractor employees, referral must be made to the Defense Industrial Security Clearance Office, DSS. The commander or security officer concerned 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 CAF of the person 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 person for denial or revocation of clearance or access to classified information if such action is warranted. No unfavorable administrative action may be taken by the organization to which the person is assigned for duty without affording the person the full range of protections outlined in section C9.2. or in the case of SCI, Annex B, DCID 6/14 (reference (k)).

C9.1.2.2. The Director, DSS, 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 DSS. DoD Components and industry will assist DSS 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.

#### C9.1.3. Suspension

C9.1.3.1. The commander or head of the organization, or Component CAF shall determine based upon receipt of derogatory information whether or not to suspend subject's access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination) until a final determination is made by the CAF.

C9.1.3.2. Whenever a determination to suspend is made, the commander or Component CAF must notify the person in writing, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.

C9.1.3.3. Component field elements must promptly report all suspension actions to the appropriate CAF via JPAS, but not later than five working days from the date of the suspension action. The adjudicative authority will immediately update JPAS access fields to alert all users to the person's changed status if not already accomplished by the field element.

C9.1.3.4. 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 CAF concerned until finally resolved. The DASD(S&IO) will monitor suspension cases pending in excess of 12 months via JPAS for appropriate action.

C9.1.3.5. A final personnel security determination shall be made for all suspension actions and the determination entered in JPAS. If, however, the person under suspension leaves the jurisdiction of DoD 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 and access fields is appropriate. In no case shall a "suspension" code (Code Y) remain as a permanent record in JPAS.

C9.1.3.6. An access entry in JPAS may be administratively downgraded based solely on the fact that a periodic reinvestigation was not initiated or completed within the five year time period for TOP SECRET/SCI or within the period prevailing for SECRET and CONFIDENTIAL clearances.

C9.1.4. Final Unfavorable Administrative Actions. Personnel security determinations that result in an unfavorable administrative action is limited to the authorities designated in Appendix 3. The authority to terminate the employment of a civilian employee is vested solely in the head of the DoD Component concerned and in such other statutory officials as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense (OSD) and DoD Components, on the basis of criteria listed in subparagraphs C2.2.1.1. to C2.2.1.3. shall be coordinated with the DASD(S&IO) 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 (non-security) 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 person for denial or revocation of a security clearance, access to classified information, or assignment to a sensitive position if warranted.

## C9.2. PROCEDURES

C9.2.1. General. No final unfavorable personnel security clearance or access determination shall be made without granting the person concerned the procedural benefits set forth in section C9.2.2. when such determination results in an unfavorable administrative action (see paragraph

C9.1.1.). As an exception, DoD contractor personnel shall be afforded the procedures contained in DoD Directive 5220.6 (reference (d)). Procedures for unfavorable decisions regarding access to SAPs may differ from the procedures in this Regulation as authorized in E.O. 12968 (reference (c)), and as approved by the Secretary of Defense or Deputy Secretary of Defense.

C9.2.2. Unfavorable Administrative Action Procedures. Except as provided for below, no unfavorable administrative action shall be taken under the authority of this Regulation unless the person concerned has been:

C9.2.2.1. 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 7, 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 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 7. In addition, the CAF will provide within 30 calendar days, upon request of the person, 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, the CAF will provide the name and address of the agency or agencies to which the individual may write to obtain a copy of the records. The head of the local organization of the person receiving an SOR shall designate a point of contact (POC) to serve as a liaison between the CAF and the subject. The duties of the POC will include, but not necessarily be limited to, delivering the SOR; having the subject acknowledge receipt of the SOR; determining whether the subject intends to respond within the time specified; ensuring that the subject understands the consequences of the proposed action as well as the consequences of failing 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 subject understands that he or she can obtain legal counsel or other assistance at his or her own expense.

C9.2.2.2. Afforded an opportunity to reply in writing to the CAF within 30 calendar days from the date of receipt of the SOR. Failure to submit a timely response could result in forfeiture of all future appeal rights with regard to the unfavorable administrative action. Exceptions to this policy may only be granted by the CAF in extraordinary circumstances where the subject's failure to respond to the SOR was due to factors beyond his and her control. The CAF must be notified of the subject's intent to respond, via the POC, within ten 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 subject. Additional extensions may only be granted by the CAF. Responses to the CAF must be forwarded through the head of the employing organization.

C9.2.2.3. Provided a written response by the CAF to any submission under subparagraph C9.2.2.2. 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 (LOD) and its enclosures at Appendix 7. 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 C9.2.2.2. provided no additional investigative action is necessary. If a final response cannot be completed within the time frame allowed, the subject 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 C9.2.2.2.

C9.2.2.4. Afforded an opportunity to appeal an LOD, issued pursuant to subparagraph C9.2.2.3. to the Component Personnel Security Appeal Board (PSAB). The PSAB shall consist of a minimum of three members and function in accordance with Appendix 8. If a decision is made to appeal the LOD, the individual may do so by one of the following methods:

C9.2.2.4.1. Appeal Without a Personal Appearance. Advise the PSAB within ten 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;

C9.2.2.4.2. Appeal With a Personal Appearance. Advise the DOHA within ten 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 notice requesting the personal appearance. Procedures governing the conduct of the personal appearance before a DOHA AJ are contained at Appendix 10.

C9.2.2.5. Provided a final written decision by the PSAB, including a rationale, to any submission under subparagraph C9.2.2.4. stating the final disposition of the appeal. This will normally be accomplished within 60 calendar days of receipt of the written appeal from the subject if no personal appearance was requested, or within 30 calendar days from receipt of the AJ recommendation if a personal appearance was requested.

C9.2.3. Reapplication. An individual is barred from reapplying for a security clearance sooner than 12 months from the date his/her security clearance was finally denied or revoked. If there is a need for access in the future, reapplication for a security clearance may be made by the individual through his/her employing activity to the appropriate CAF. The individual is responsible for providing the CAF with documentation that the circumstances or conditions that resulted in denial or revocation have been rectified or sufficiently mitigated to warrant reconsideration. The CAFs have the authority to accept or reject the reapplication.

C9.2.4. Exceptions to Policy. Notwithstanding paragraph C9.2.2. 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 Title 5 U.S.C. 7532 (reference (kk)). Such authority may not be delegated and may be exercised only when it is determined that the

procedures prescribed in paragraph C9.2.2. are not appropriate. Such determination shall be conclusive.

### C9.3. REINSTATEMENT OF CIVILIAN EMPLOYEES

C9.3.1. A DoD civilian employee terminated under the provisions of this Regulation shall not be reinstated, restored to duty or reemployed in the Department of Defense unless the Secretary of Defense or the head of a DoD Component finds doing so is clearly consistent with the interests of national security. Such a finding shall be made part of the personnel security record.

C9.3.2. Reinstatement Benefits. A DoD civilian employee whose employment was suspended or terminated under the provisions of this Regulation and who is reinstated or restored to duty under the provisions of Title 5 U.S.C. 3571(reference (ll)) is entitled to benefits as provided for by Title 5, U.S. C. 652 (a), (b), (c). (reference (mm)).

## C10. CHAPTER 10

### CONTINUING SECURITY RESPONSIBILITIES

#### C10.1. EVALUATING CONTINUED SECURITY ELIGIBILITY

C10.1.1. A personnel security determination is an effort to assess the future trustworthiness of a person in terms of the likelihood of the person 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 person's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the person's supervisor, co-workers, and, to a large degree, the person himself and herself. 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.

##### C10.1.1.1. Management Responsibility

C10.1.1.1.1. Commanders and heads of organizations shall ensure 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 implications of their duties and on their individual responsibilities.

C10.1.1.1.2. The heads of DoD Components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who have questions or concerns about financial matters, mental health, or substance abuse that may affect their eligibility for access to classified information. 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.

C10.1.1.2. Supervisory Responsibility. Security programs shall be established to ensure that supervisory personnel are familiar with their personnel security responsibilities. These programs are to provide practical guidance as to indicators of personnel security concern. Specific instructions should be disseminated on reporting procedures to enable timely corrective action to protect the interests of national security and to provide necessary help to the person to correct any personal problem which may affect the person's continued eligibility for access or occupancy of a sensitive position.

C10.1.1.2.1. Supervisors are not to review the security forms of anyone undergoing a periodic reinvestigation. Supervisory knowledge of any significant adverse information is to be independent of the information reflected on the security form.

C10.1.1.3. Individual Responsibility

C10.1.1.3.1. Personnel must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, they must be aware of the standards of conduct required of persons holding positions of trust. In this connection, they 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.

Moreover, personnel having access to classified information shall:

C10.1.1.3.1.1. Protect classified information in their custody from unauthorized disclosure;

C10.1.1.3.1.2. Report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

C10.1.1.3.1.3. Report all violations of security regulations to the appropriate security officials;

C10.1.1.3.1.4. Comply with all other security requirements.

C10.1.1.3.1.5. Report any information of the type referenced in Appendix 5.

C10.1.1.4. Co-worker Responsibility. Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

C10.2. SECURITY EDUCATION

C10.2.1. General. The effectiveness of a person in meeting security responsibilities is proportional to the degree to which that person understands them. Thus, an integral part of the DoD security program is the indoctrination of personnel 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.

C10.2.2. Initial Briefings. All persons cleared for access to classified information or assigned to sensitive duties under this Regulation shall be given an initial security briefing. The

briefing shall be in accordance with the requirements of DoD 5200.1-R (reference (u)) or DCID 6/4 (reference (k)) as applicable. If a person declines to execute Standard Form 312, "Classified Information Nondisclosure Agreement", the DoD Component shall initiate action to deny or revoke the security clearance of such person in accordance with section C9.2. In addition to the SF 312, if a person declines to execute an SCI Nondisclosure Agreement, action must be initiated to deny SCI access.

C10.2.3. 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 DoD 5200.1-R (reference (u)) or DCID 6/4 (reference (k)) as applicable, shall be tailored to fit the needs of the personnel.

C10.2.4. Foreign Travel Briefing. The DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security office when any person attempts to acquire by unauthorized means information related to the national defense as outlined in DoD Instruction 5240.6 (reference (nn)). Additionally, personnel with SCI access must report their travel itinerary per DCID 1/20 (reference (oo)).

C10.2.5. Termination Briefing. DoD military personnel and civilian employees who terminate employment or whose clearance is terminated or who contemplate an absence from duty or employment for 60 days or more, shall be given a termination briefing. The briefing shall be in accordance with the requirements of DoD 5200.1-R (reference (u)) or DCID 6/4 (reference (k)).

## C11. CHAPTER 11

### INVESTIGATIVE RECORDS

#### C11.1. SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS

C11.1.1. General. In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is DoD 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 suitability for or retention in employment; determining eligibility 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 and other uses authorized by the Privacy Act (reference (pp)). Uses such as promotion, selection and retention in the Military Services, are subject to the specific written authorization of the DASD(S&IO).

C11.1.2. 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 shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records.

C11.1.3. Access Restrictions. Access to personnel security investigative reports and personnel security clearance determination information shall be authorized only in accordance with DoD Regulations 5400.7-R and 5400.11-R (references (ii) and (jj), respectively) and with the following:

C11.1.3.1. 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 provided it complies with the purposes stated in subparagraph C11.1.1. and is to an agency authorized to receive it for that purpose.

C11.1.3.2. Within the DoD, 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 subparagraph C11.1.1.

C11.1.3.3. Access by subjects of personnel security investigative reports shall be given such access as is authorized under DoD Directive 5400.11-R (reference (jj)), or if greater access is provided, under DoD 5400.7-R (reference (ii)).

C11.1.3.4. Access to personnel security clearance determination information shall be made available, other than provided for in subparagraph C11.1.3. only to the DoD or other officials of the Federal Government who have an official need for such information.

C11.1.3.5. If an individual requests access to his and her personnel security investigative reports and declines to have his or her signature notarized, an unsworn declaration, certificate, verification or statement subscribed to as true under penalty of perjury will be accepted in lieu of a notarized signature.

C11.1.3.5.1. If executed within the United States, its territories, possessions, or commonwealth, it shall read as follows: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct." Executed on (date). (Signature)

C11.1.3.5.2. If executed outside the United States, it shall read as follows: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct." Executed on (date). (Signature)

C11.1.4. Safeguarding Procedures. Personnel security investigative reports and personnel security determination information shall be safeguarded as follows:

C11.1.4.1. Authorized requesters shall control and maintain accountability of all reports of investigation received.

C11.1.4.2. 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.

C11.1.4.3. Personnel security investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lockbar and an approved three-position dial-type combination padlock or in a similarly protected area and/or container.

C11.1.4.4. 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:

TO BE OPENED ONLY BY OFFICIALS DESIGNATED TO  
RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATIONS

C11.1.4.5. A person's status with respect to a personnel security clearance or SCI or SAP access is to be protected as provided for in DoD 5400.7-R (reference (ii)).

C11.1.4.6. As reports of investigation begin to be provided electronically, CAFs shall establish procedures and safeguards to control and maintain reports of investigation received in this manner.

#### C11.1.5. Records Disposition.

C11.1.5.1. Personnel security investigative reports, to include OPM NACIs and ANACIs, 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 DoD 5200.1-R (reference (u)).

C11.1.5.2. DoD record repositories authorized to file personnel security investigative reports shall destroy PSI reports of a favorable or of a minor derogatory nature 15 years after the date of the last investigative action. That is, an investigative update, special investigative inquiry, or any other investigative activity that causes information to be added to the file. 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 in the investigation shall be destroyed 25 years after the date of the last investigative 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.

C11.1.5.3. Personnel security investigative reports on persons who are considered for affiliation with DoD will be destroyed after two years if the affiliation is not completed. The employing agency or service shall notify the investigative provider in such instances to ensure compliance with this requirement.

C11.1.6. Foreign Source Information. Information that is classified by a foreign government is exempt from public disclosure under the Freedom of Information and Privacy Acts (references (ii) and (jj)). 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.

## C12. CHAPTER 12

### AUTOMATED SYSTEMS

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

##### C12.1.1. General

C12.1.1.1. DCII is an automated central repository that identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities. The DCII data base consists of an 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 determinations are maintained in the DCII by subject. DoD investigative and adjudicative authorities report information that is used for investigative, adjudicative, statistical, research and other purposes as authorized by DASD(S&IO) approval.

C12.1.1.2. The DCII will be replaced as the authoritative clearance and access database for the Department when JPAS becomes fully operational. It will continue as the central index of investigations for the Department.

C12.1.2. Access. The DCII is operated and maintained by DSS on behalf of the DoD Components and the DASD(S&IO). Access is normally limited to DoD 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 below. On approval, a Memorandum of Understanding (MOU) addressing equipment, maintenance, security, privacy, and other agency responsibilities shall be forwarded to the requester by DSS for signature.

C12.1.2.1. Military Departments and Defense Agencies. Military Departments and Defense Agencies shall establish policy and procedures and serve as the approval authority for activities within their organization wishing to gain access to the DCII. On approval, the requests shall be forwarded to DSS for implementation.

C12.1.2.2. Non-DoD Agencies. Requests from Non-DoD Agencies must be submitted to DASD(S&IO), ATTN: Director, Security, Room 1E775, 6000 Defense, Pentagon, Washington, D.C. 20301-6000. On approval, these requests will be forwarded to DSS for implementation.

C12.1.2.3. OPM Security-Suitability Investigations Index (SII). Authorized DCII users will be able to obtain a "read only" search of the SII at the same time that they are conducting a search of the DCII. The minimum investigative requirement for "read only" access is a favorably completed NACLIC or NACLIC/PR, current within ten years.

C12.1.3. Investigative Data.

C12.1.3.1. Contributors to the DCII shall ensure that all personal investigative and clearance and access data entered into the DCII is accurate, relevant, timely, and complete.

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, 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.

C12.1.3.5. Open or pending criminal investigations will be "masked" and available only to certain DoD and non-DoD investigative and adjudicative authorities upon direction of the Defense Criminal Investigative Organizations (DCIO).

C12.1.4. Adjudicative Data. Ninety days after JPAS reaches initial operating capability, all adjudicative determinations on personnel with access to classified information or performing sensitive duties shall be entered only in JPAS. In the meantime, guidance regarding DCII entries remains unchanged. In the future, this guidance will also pertain to JPAS entries.

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

C12.1.4.1.1. Suspension of access.

C12.1.4.1.2. Issuance of interim access by the CAF or employing activity.

C12.1.4.1.3. Granting, denial, or revocation of a clearance or access.

C12.1.4.1.4. Following 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 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 DoD. The determination may be deleted two years after the employment and/or clearance eligibility ends. The deleted DCII data shall be retained by the DSS in a historical file for a minimum of five 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.

C12.1.4.6. A DCII clearance or access entry may be used as the primary basis for granting immediate access to the equivalent level of information, without further adjudication provided:

C12.1.4.6.1. The investigation is current.

C12.1.4.6.2. A favorable clearance/access determination by a DoD CAF is present.

C12.1.4.6.3. No subsequent investigations are present.

C12.1.4.6.4. A DCII investigative tracing may not be used as the basis for an unfavorable adjudicative determination.

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 applicable federal information system security standards. Contributors may enter only unclassified information.

C12.1.6.2. Information contained in the DCII receives the protection required by the Privacy Act.

C12.1.6.3. Due to the sensitive nature of the information, personnel authorized to input, modify, or delete data entered into the DCII must have a favorably completed SSBI or SSBI/PR, current within five years.

C12.1.6.4. Personnel from DoD activities and other Federal Agencies that have been authorized "Read Only" access to the DCII must have a favorably completed NACLIC, NACLIC/PR or NACI, current within ten years.

C12.1.6.5. A favorably completed SSBI or SSBI/PR, current within five years, is required for all persons requesting, handling, or reviewing investigative files.

C12.1.6.6. 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.

C12.1.6.7. 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.

C12.1.6.8. When the DCII terminal is operational, access to DCII information shall be controlled and limited to those persons authorized access to that information.

C12.1.6.9. All authorized DCII users, both DoD and non-DoD, must annually recertify to the DSS Director for Information Services, the names, SSN's, DPOB, date and type of their last investigation. Failure to do so will result in cancellation of DCII access privileges.

C12.1.7. Disclosure of Information. The Privacy Act (reference (pp)) requires an accounting of the disclosure of personal information when it is provided to another Agency. For accessing the DCII, DoD is considered a single Agency. Disclosure of personal information within the Department of Defense to those officials or employees who have a need for the information in the performance of their duties 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 released 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 unless the requester also requests access under the Freedom of Information Act and greater access would thereby be provided.

## C12.2. JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

### C12.2.1. Definition, Roles and Responsibilities

C12.2.1.1. JPAS is the DoD personnel security clearance and access database. It facilitates personnel security management for the DoD CAFs, security managers and officers both non-SCI and SCI functions. It interfaces with the investigative providers, the personnel systems within the Department and DMDC thus eliminating manual transactions and expediting the flow of personnel security information to warfighters. JPAS is operated and maintained by the Air Force on behalf the DoD Components and ASD(C3I).

C12.2.1.2. JPAS has two applications. The Joint Adjudication Management System (JAMS) and the Joint Clearance and Access Verification System (JCAVS). JAMS is for adjudicative personnel only and provides capabilities such as case management/distribution, adjudication history and summary, due process, revocations, and denial actions, and the ability for each CAF to electronically access investigative reports from the investigative providers. JCAVS is for non-SCI and SCI security managers/officers and provides capabilities such as access indoctrination/debriefing history, incident/issue file reporting and history, SAP access information, and management of unit personnel security functions.

C12.2.1.3. JCAVS users will be responsible for changes to individual accesses. This includes initials, upgrades, downgrades, suspensions, and access no longer required. JCAVS

users will input the following access codes in JPAS that will also update the DCII via the CAF daily maintenance updates within 24 hours.

C-Confidential	S-Secret	T-Top Secret
V-SCI Compartments	E-Interim Confidential	O-Interim Secret
P-Interim Top Secret	U-Interim SCI	Y-Access Suspended

C12.2.1.4. JCAVS users are authorized upon favorable review of JPAS records to grant access to individuals under their security cognizance. CAFs reserve the right to rescind any access decision made by the field JCAVS users. Access may be granted under the following conditions if the individual's record indicates:

- C12.2.1.4.1. A current investigation,
- C12.2.1.4.2. A valid clearance eligibility at the required level,
- C12.2.1.4.3. No break in service longer than 24 months,
- C12.2.1.4.4. No investigation or other information subsequent to the date of eligibility is indicated, and
- C12.2.1.4.5. No "exception" is indicated in the JPAS record.

C12.2.2. System of Record. JPAS is the DoD system of record for personnel security adjudication, clearance and access verification and history. DoD Components and cleared DoD contractor facilities will access this system.

C12.2.3. Access to JPAS. The following are the minimum investigative standards required for access to JPAS.

C12.2.3.1. JAMS. SSBI or SSBI-PR. This authorizes read and write capability to all DoD personnel security records.

C12.2.3.2. JCAVS. Encompasses six user levels with varying duties and responsibilities associated to each level.

C12.2.3.2.1. User Levels 2, 3, 4 and 5. SSBI or SSBI-PR. This authorizes read and write capability.

C12.2.3.2.2. User Levels 6 and 7. NACL/ANACI or PR equivalent. This authorizes read only capability.

C12.2.3.3. JPAS Database Administrator/System administrator/Account Manager. SSBI or SSBI-PR. Individuals occupying IT positions must also meet the requirements for IT Level 1.

#### C12.2.4. JCAVS User Levels.

C12.2.4.1. CAF System Administrator/Database Manager. Individual responsible for establishing all JAMS accounts and liaison with DoD Agency/MILDEP/Unified Command Account Administrator and JCAVS System Administrator. Read access only.

C12.2.4.2. DoD Agency/MILDEP/Unified Command Account Administrator. Designated by SOIC/SOIC designee or Senior Security Official to appoint primary and alternate account managers (all levels); approve/disapprove system access request for designated user levels (including dual-hatted organizations) for JCAVS system administrator; maintain analysis of user level accounts to determine trends; report/resolve problems (network, communications, etc.); liaison with CAF system administrator/database manager, etc., and Primary point-of-contact for JCAVS Customers. Read access to organization personnel only.

C12.2.4.3. User Level 2. SCI Security Personnel at HQ Unified Command, HQ DoD Agency, or HQ MILDEP Major Command. Span of Control is determined by responsible SOIC or Designee, generally approval authority for SCI security matters per DoD 5105.21 (reference (qq)).

C12.2.4.4. User Level 3. SCI Security personnel at echelons subordinate to Level 2, in a particular geographic location (installation, post, base, naval vessel) responsible for providing SCI security support to multiple organizations, including those across different organizational lines. Span of Control is determined by responsible SOIC or designee per DoD 5105.21 (reference (qq)).

C12.2.4.5. User Level 4. Non-SCI security personnel at HQ Unified Command, HQ DoD Agency, or HQ MILDEP Major Command. Responsible Senior Security Official determines Span of Control.

C12.2.4.6. User Level 5. Non-SCI security personnel at echelons subordinate to Level 4, in a particular geographic location (installation, post, base, naval vessel) responsible for non-SCI security support to multiple organizations, including those across different organizational lines. Responsible Senior Security Official determines Span of Control.

C12.2.4.7. User Level 6. Unit Security Manager (Additional Duty) responsible for security functions as determined by responsible Senior Security Official.

C12.2.4.8. User Level 7. Entry Control Personnel. Individuals who grant access to installation, buildings, etc. Varies according to organizations.

#### C12.2.5. Data Transfer/Data Retention.

C12.2.5.1. Data Transfer will be accomplished in JPAS for both military and civilian personnel security records. This entails all entries completed by both JAMS and JCAVS User and will be viewable to the respective user populous. The "Total Person Concept" will be applicable for all data transfers, thus, access information for both non-SCI and SCI will be

included in transfers. The availability and update of this information will be determined on input received from the personnel system. For instance, debriefing of access will be accomplished prior to the data transfer, thus eliminating the need for transfer-in-status actions.

C12.2.5.2. Data will be permanently retained within JPAS but it will not always be displayed. Data pertaining to individuals that retire or separate from the DoD will be visibly retained for 24 months. However, if no action occurs on the individual record it will be purged from display and archived. Retrieval of archival data will be authorized with written consent and 72 hours notification to the JPAS Personnel Management Office (PMO). General Officer and Senior Executive Service data will be visibly retained indefinitely or upon notification from the appropriate MILDEP/DoD Agency that visual display is no longer required.

## C13. CHAPTER 13

### PEER REVIEW

#### C13.1. GENERAL

This Chapter establishes the procedures for the review of all DoD CAFs on a triennial basis to ensure the CAF is able to perform its functions efficiently and effectively and the rights of the individual are protected.

#### C13.2. OBJECTIVES OF REVIEW SYSTEM

The review should assess:

C13.2.1. The quality and consistency of adjudicative decisions and work products.

C13.2.2. Whether or not the CAF has sufficient resources to perform its mission.

C13.2.3. The procedures and metrics to measure CAF performance.

#### C13.3. CAF PARTICIPATION

C13.3.1. CAF reviews will be conducted, at a maximum, on a triennial basis, with three CAF reviews conducted each year. The review team will be comprised of 2-4 senior adjudicators/managers (GS-13-15) from other CAFs, one of who may be a CAF chief. The senior team member will act as the team leader. Size of the team will vary according to the size of the CAF to be reviewed. When an SCI CAF is to be reviewed, DIA will head the team.

C13.3.2. The review will consist of a data call, site visit and written report by the review team. All CAFs are required to provide the information requested in the data call. Appendix 11 outlines the structure of the data call and a suggested schedule for reviews and team membership.

C13.3.3. The team leader is responsible for scheduling the review and forming the review team. The team leader is to ensure that the inspected CAF receives the data call no less than 60 days prior to the site visit. The completed information is to be returned to the team leader no less than 3 weeks before the site visit. Results of the data call are to be reviewed by the team prior to the site visit. The site visit should not be more than one week.

C13.3.4. The CAF under review will provide all information and materials requested and work space for the team to utilize during the site review.

#### C13.4. AREAS OF REVIEW

The following areas are to be reviewed to determine how the CAF is performing its mission:

C13.4.1. Cost Effectiveness/Resources. Organizational structure, budget and staffing, and training shall be reviewed to ascertain if the CAF has sufficient resources to perform its mission.

C13.4.2. Efficiency. Production of the CAF and the automation available to assist the CAF in accomplishing its mission.

C13.4.3. Operational Procedures. CAF procedures and metrics to measure CAF performance.

C13.4.4. Standardization. CAF procedures to ensure determinations are consistent with standards.

C13.4.5. Individual rights versus National Security. Procedures for denying or revoking eligibility to ensure fair and equitable treatment.

C13.4.6. Other review. Any other areas identified through audits, previous reviews, Component self-inspections, or that arise during the course of the review.

### C13.5. STRUCTURE OF THE REVIEW

C13.5.1. The team leader will structure the review to ensure all areas of review are accomplished. The team leader may assign team members areas of responsibility during the site visit.

C13.5.2. A suggested framework for the review:

C13.5.2.1. Notification of review, in and out briefs with CAF chief and immediate superior organization

C13.5.2.2. Assessment and validation of information generated by the data call

C13.5.2.3. Review of CAF policies; procedural manuals; performance measures; work accounting procedures; and sampling of clean, minor issue, major issue, compelling need, SOR, and due process cases, and waivers.

C13.5.2.4. Observation of CAF processes to include case opening, review, adjudication, JPAS entry, and recording of adjudicator justification of decision to include mitigation rationale.

### C13.6. ACTIONS AS A RESULT OF REVIEW

The team will generate a written report of its review for DASD(S&IO), the concerned CAF and its immediate superior organization within 45 days after completion of the review. A copy of the report on SCI CAFs and any corrective actions will also be provided to DIA. The report should contain, if warranted, recommendations that would benefit the adjudicative community. For standardization and improvement to occur, there must be information sharing and training components. DASD(S&IO) will periodically apprise CAFs and adjudicative training entities of best practices discovered, deficiencies noted, and other recommendations for the betterment of the adjudicative community. Deficiencies and adverse findings will not be attributed to specific CAFs.

## AP1. APPENDIX 1

### INVESTIGATIVE STANDARDS FOR BACKGROUND INVESTIGATIONS FOR ACCESS TO CLASSIFIED INFORMATION

The content of this Appendix is taken verbatim from the Investigative Standards approved by the President in March 1997. On December 17, 2001, the Personnel Security Working Group of the Records Access and Information Security Policy Coordinating Committee provided clarification of the national standards with regard to the conduct of CIA Directorate of Operations Records Checks, source coverage for the SSBI-PR, and local agency check coverage. These changes have been incorporated into the investigative standards. Italicized type is used to denote how the standards in certain areas will be implemented within DoD.

#### 1. INTRODUCTION

The following investigative standards have been established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs), and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

#### 2. THE THREE STANDARDS

There are three standards (Table 1 summarizes when to use each one):

- a. The investigation and reinvestigation standard for "L" access authorizations and for access to Confidential and Secret (including all Secret-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by Section 4.4 of Executive Order 12958);
- b. The investigation standard for "Q" access authorizations and for access to Top Secret (including Top Secret SAPs) and SCI; and
- c. The reinvestigation standard for continued access to the levels listed in paragraph 2(b).

#### 3. EXCEPTIONS TO PERIODS OF COVERAGE

Some elements of standards specify a period of coverage (e.g., seven years). Where appropriate, such coverage may be shortened to the period from the subject's 18th birthday to the present or to two years, whichever is longer.

*However, no investigation shall be conducted prior to an individual's 16th birthday. Additionally, lack of coverage in any investigative category shall be compensated for through other investigative means.*

#### 4. EXPANDING INVESTIGATIONS

Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and Executive Orders.

#### 5. TRANSFERABILITY

Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements for all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

#### 6. BREAKS IN SERVICE

If a person who requires access has been retired or separated from U.S. Government employment for less than two years and is the subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated SF 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968 (see Table 2).

#### 7. THE NATIONAL AGENCY CHECK (NAC)

The National Agency Check is a part of all investigations and reinvestigations. It consists of a review of

*The scope for the NAC is five years or to age 18, whichever is the shorter period.*

:

- a. Investigative and criminal history files of the FBI, including a technical fingerprint search;

1. *FBI/HQ has on file copies of investigations conducted by the FBI. The FBI/HQ check consists of a review of files for information of a security nature and that are developed during applicant-type investigations.*

2. *FBI/ID check is based upon a technical fingerprint search that consists of a classification of the subject's fingerprints and a 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.*

- b. OPM's Security/Suitability Investigations Index (SII);

*The files of OPM contain the results of investigations conducted by OPM under Executive Order 10450, those requested by the NRC, the DOE, and those requested since August 1952 to serve as a basis for "Q" clearances. Additionally, personnel security adjudicative*

*determinations rendered by other federal agencies are contained in the SII. OPM SII records shall be checked on all subjects of DoD investigations.*

- c. DoD's Defense Clearance and Investigations Index (DCII); and
- d. Such other national agencies (e.g., CIA, INS) appropriate to the individual's background.

1. Central Intelligence Agency (CIA).

a. Directorate of Operations (CIA-DO). This database shall be checked on all non-U.S. citizen spouses, cohabitants, and immediate family members, whether or not they reside in the United States. *In addition, this database shall be queried on the subject any time there is a counterintelligence concern raised during the conduct of the PSI.*

b. Office of Security (CIA-OS) 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 the CIA may have pertinent information.*

2. 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 declarations of intention, visitor's visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the United States. I&NS records are checked when the subject is:*

- a. *An alien in the U.S., or*
- b. *A naturalized citizen whose naturalization has not been verified, or*
- c. *An immigrant alien, or*
- d. *A U.S. citizen who received derivative citizenship through the naturalization of one or both parents provided that such citizenship has not been verified in a prior investigation.*

3. State Department. *The State Department maintains the following records:*

a. *Security Division files contains 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.*

b. *Passport Division files 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/she was born. Verification of this registration is verification of citizenship.*

4. Military Personnel Record Center (MPRC). 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.

Military requesters must review service records of any active duty member at the time the investigation is requested. Unfavorable information must be recorded on the investigative request form. Review of prior military service records is to be conducted by the investigating agency through the Defense Manpower Data Center databases or the Military Personnel Record Center files, as appropriate.

5. Treasury Department. The files of Treasury Department agencies (Secret Service, Internal Revenue Service and Bureau of Customs) shall be checked only when available information indicates that an agency of the Treasury Department may be reasonably expected to have pertinent information.

6. The files of other agencies such as the National Guard Bureau, etc. shall be checked when pertinent to the purpose for which the investigation is being conducted.

## STANDARD A

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

#### 8. Applicability.

Standard A applies to investigations and reinvestigations for:

- a. Access to Confidential and Secret (including all Secret-level SAPs) not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section 4.4, E.O. 12958) and
- b. "L" access authorizations.

#### 9. For Reinvestigations: When to Reinvestigate.

The reinvestigation may be initiated at any time following completion of, but not later than ten years (fifteen years for Confidential) from the date of, the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation including when there has been a break in service.).

#### 10. Investigative Requirements:

- a. Completion of Forms: Completion of Standard Form 86 including applicable releases and supporting documentation;

- b. National Agency Check: Completion of a National Agency Check.

*For Secret and Confidential periodic reinvestigations, fingerprint cards are not required if there is a previous valid technical check of the FBI.*

- c. Financial Review: Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

- d. Date and Place of Birth: Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

*Verification of date and place of birth by sighting an original or certified copy of a birth certificate or other acceptable documentation should normally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance. If a variance or discrepancy in the documentation provided exists, the request for investigation should be annotated to this effect.*

- e. Local Agency Checks: As a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last five years, and, if applicable, of the appropriate agency for any identified arrests. Checks of court records, state criminal history files, or other appropriate records are appropriate where local agency checks are refused, or involve extensive delays or large fees.

## 11. Expanding Investigations.

The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

## STANDARD B

### **Single Scope Background Investigation (SSBI)**

## 12. Applicability.

Standard B applies to initial investigations for:

- a. Access to Top Secret (including Top Secret SAPs) and SCI; and
- b. "Q" access authorizations.

## 13. Investigative Requirements.

Investigative requirements are as follows:

- a. Completion of Forms: Completion of Standard Form 86, including applicable releases and supporting documentation;
- b. National Agency Check: Completion of a National Agency Check.
- c. National Agency Check for the Spouse or Cohabitant (if applicable): Completion of National Agency Check, without fingerprint cards, for the spouse or cohabitant.
- d. Date and Place of Birth: Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

*Verification of date and place of birth by sighting an original or certified copy of a birth certificate or other acceptable documentation should normally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance. If a variance or discrepancy in the documentation provided exists, the request for investigation should be annotated to this effect.*

- e. Citizenship: For individuals born outside the United States, verification of U.S. citizenship directly from the appropriate registration authority; verification of U.S. citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

*Verification of citizenship by sighting of acceptable documentation should normally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance. If a variance or discrepancy in the documentation provided exists, the request for investigation should be annotated to this effect. For individuals born outside the U.S., the investigating agency will verify citizenship directly from the appropriate registration authority and also, verify U.S. citizenship or legal status of foreign-born immediate family members over the age of 18.*

*Acceptable proofs of citizenship are as follows:*

1. *For individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar's signature. It must bear the raised, impressed, or multicolored seal of the registrar's office. The only exception is a state or other jurisdiction that does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable.*

2. *A delayed birth certificate is one created when a record was filed more than one year after the date of birth. Such a certificate is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include: baptismal or circumcision certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of birth. Other documentary evidence can be early census, school, or family bible records, newspaper files, or insurance papers.*

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

4. *If the individual claims citizenship by naturalization, a certificate of naturalization shall be submitted.*

5. *If citizenship was acquired by birth abroad to a U.S. citizen parent or parents, the following are acceptable evidence:*

a. *A Certificate of Citizenship issued by the Immigration and Naturalization Service;*  
*or*

b. *A Report of Birth Abroad of a Citizen of the United States of America (Form FS-240); or*

c. *A Certificate of Birth (Form FS-545 or DS-1350).*

d. *A passport or one in which the individual was included will be acceptable.*

f. **Education:** Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education was a primary activity of the subject during the most recent three years.

*Corroboration of education within the scope of investigation shall normally be accomplished by the requester prior to the initiation of the request for investigation. If all education is outside of the investigative scope, the last education above high school level will be verified.*

g. **Employment:** Verification of all employment for the past seven years; personal interviews of sources (supervisors, coworkers, or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior federal and military service, including type of discharge. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments. *However, each duty location must be listed.*

*For Federal employees, all service within one agency of the Federal Government will be considered as one employment, regardless of assignment. However, each duty location must be listed.*

h. **References:** Four references, of whom at least two are developed; to the extent

practicable, all should have social knowledge of the subject and collectively span at least the last seven years.

i. Former Spouse: An interview of any former spouse divorced within the last ten years.

j. Neighborhoods: Confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

*The SSBI standard for neighborhoods allows an investigative entity sufficient flexibility to meet the standard, provided that a reasonable effort is made to obtain coverage within the investigative period and the lack of coverage in any investigative category should be compensated for through other investigative means.*

k. Financial Review: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the last seven years.

l. Local Agency Checks: A check of appropriate criminal history records covering all locations where, for the last ten years, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (NOTE: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.) Checks of court records, state criminal history files, or other appropriate records are appropriate where local agency checks are refused, or involve extensive delays or large fees.

m. Public Records: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject.

n. Subject Interview: A subject interview conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

o. Polygraph (only in agencies with approved personnel security polygraph programs): In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

#### 14. Expanding the Investigation

The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

## STANDARD C

### **Single Scope Background Investigation Periodic Reinvestigation (SSBI-PR)**

#### 15. Applicability

Standard C applies to reinvestigations for

- a. Access to Top Secret (including Top Secret SAPs) and SCI; and
- b. "Q" access authorizations

#### 16. When to Reinvestigate

The reinvestigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation. (See Table 2).

*The investigation will cover the most recent five year period or the period since the last investigation, whichever is shorter.*

#### 17. Reinvestigative Requirements

Reinvestigative requirements are as follows:

- a. Completion of Forms: Completion of Standard Form 86, including applicable releases and supporting documentation.
- b. National Agency Check: Completion of a National Agency Check (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).
- c. National Agency Check for the Spouse or Cohabitant (if applicable): Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant. The National Agency Check for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.
- d. Employment: Verification of all employment since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employment of six months or more. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

*For Federal employees, all service within one agency of the Federal Government will be considered as one employment, regardless of assignment.*

- e. References: Interviews with two character references who are knowledgeable of the subject; at least one will be a developed reference. To the extent practicable, both should have social knowledge of the subject and collectively span the entire period of the reinvestigation. As

appropriate, additional interviews may be conducted, including with cohabitants and relatives. Assuming otherwise adequate coverage, one individual can qualify as a source in more than one category, i.e. neighborhood, employment, or character.

f. Neighborhoods: Interviews of two neighbors in the vicinity of the subject's most recent residence of six months or more. Confirmation of current residence regardless of length.

*The SSBI-PR standard for neighborhoods allows any investigative entity sufficient flexibility to meet the standard, providing that a reasonable effort is made to obtain coverage within the investigative period and that lack of coverage in any investigative category should be compensated for through other investigative means.*

g. Financial Review.

(1) Financial Status: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(2) Check of Treasury's Financial Database: Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated databases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under \$10,000 that are reported as possible money laundering violations.

h. Local Agency Checks: A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (NOTE: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.) Checks of court records, state criminal history files, or other appropriate records are appropriate where local agency checks are refused, or involve extensive delays or large fees.

i. Former Spouse: An interview with any former spouse unless the divorce took place before the date of the last investigation or reinvestigation.

*An interview will be conducted with any former spouse whose divorce from Subject took place after the date of the last investigation or reinvestigation (regardless of how long the interval).*

j. Public Records: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.

k. Subject Interview: A subject interview conducted by a trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

## 18. Expanding the Reinvestigation

The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

## DECISION TABLES

TABLE 1: WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investigation required is	Using standard
CONFIDENTIAL SECRET	None	None	NACLCL	A
	CONFIDENTIAL SECRET, "L"	Out of date NACLCL or SSBI; NAC, ANACI, ENTNAC, NACI, BI, SBI		
TOP SECRET, SCI, "Q"	None	None	SSBI	B
	None, CONFIDENTIAL, SECRET, "L"	Current or out of date NACLCL, NAC, ANACI, ENTNAC, ANACI, NACI, SBI, BI		
	TS, SCI, "Q"	Out of date SSBI	SSBI-PR	C

TABLE 2: REINVESTIGATION REQUIREMENTS

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service or employment of		<i>Type required if there has been a break in access (no access/lower level of access) but remains in military service, federal service, or with same employer in industry</i>
		0-23 months	24 months or more	
CONFIDENTIAL	0 to 14 yrs. 11 mos.	None (Note 1)	NACLCL	None
	15 yrs. or more	NACLCL-PR		NACLCL-PR
SECRET, "L"	0 to 9 yrs. 11 mos.	None (Note 1)	NACLCL	None
	10 yrs. or more	NACLCL-PR		NACLCL-PR
TOP SECRET, SCI, "Q"	0 to 4 yrs. 11 mos.	None (Note 1)	SSBI	None
	5 yrs. or more	SSBI-PR		SSBI-PR

Note 1: As a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation (NACLCL-PR or SSBI-PR) is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968.

*DoD personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and who have a prior security clearance eligibility, will not require a NACLCL to maintain their Secret or Confidential clearance. However, personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and no prior security clearance eligibility, will require a NACLCL for issuance of a Secret or Confidential clearance, regardless of the age of the investigation.*

## Investigative Standards for Temporary Eligibility for Access

### 1. Introduction.

The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, "Access to Classified Information", are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

### 2. Temporary Eligibility for Access.

Based on a justified need meeting the requirements of section 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation

### 3. Temporary Eligibility for Access at the Confidential and Secret levels and Temporary Eligibility for "L" Access Authorization.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency with Local Agency Checks and Credit (NACLC). *A DCII check will be conducted.*

### 4. Temporary Eligibility for Access at the Top Secret and SCI levels and Temporary Eligibility for "Q" Access Authorization: For Someone who is the Subject of a Favorable Investigation Not Meeting the Investigative Standards for Access at Those Levels.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for Single Scope Background Investigation (SSBI).

### 5. Temporary Eligibility for Access at the Top Secret and SCI Levels and Temporary Eligibility for "Q" Access Authorization: For Someone who is not the Subject of a Current, Favorable Personnel or Personnel-Security Investigation of Any Kind.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited Single Scope Background Investigation (SSBI), and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal

Bureau of Investigation and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).

6. Additional Requirements by Agencies. Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968. Temporary eligibility for access is valid only at the agency granting it and at other agencies that expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968, Access to Classified Information.

## 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 investigations must ensure that continuing command attention is given to the investigative request process.

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 personnel who, under the provisions of this Regulation, have already met the security standard;

AP2.1.2. Ensure that military and civilian personnel on whom investigative requests are initiated will have at least 12 months remaining in service after completion of the investigation to warrant conducting it;

AP2.1.3. Ensure that request forms and prescribed documentation are properly executed in accordance with instructions of the investigative provider;

AP2.1.4. Dispatch the request directly to the investigative provider;

AP2.1.5. Promptly notify the investigative provider if the investigation 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 investigative provider to operate more efficiently and permit more effective, timely, and responsive service in accomplishing investigations.

#### AP2.2. REQUEST PROCEDURES

##### AP2.2.1. Investigative forms

AP2.2.1.1. Standard Form 86, (Questionnaire for National Security Positions) shall be used for personnel requiring access to classified information, enlistment in the military, assignment to sensitive positions, and as specified in this Regulation.

AP2.2.1.2. Standard Form 85P, (Questionnaire for Public Trust Positions) shall be used for personnel whose duties do not require access to classified information, but actions could cause harm to the U.S. government.

AP2.2.1.3. Standard Form 85, (Questionnaire for Non-Sensitive Positions) shall be used for entry into government service to determine if the individual can do the job and whose duties will not require access to classified information.

#### AP2.3.1. Investigative Providers

AP2.3.1.1. Defense Security Service (DSS). All investigative requests must be submitted electronically via the Electronic Personnel Security Questionnaire (EPSQ) or its successor. Instructions for downloading, completing, and submitting the EPSQ can be obtained on-line from DSS at [www.dss.mil/epsq](http://www.dss.mil/epsq). Releases and fingerprint cards are to be mailed to:

National Agency Records Process Group (NARP)  
Defense Security Service  
601 10<sup>th</sup> Street, Suite 125  
Fort George G Meade MD 20755-5134

AP2.3.1.2. Office of Personnel Management (OPM). Currently, all investigative requests are to be completed in hard copy and mailed to OPM. OPM will accept a hard copy EPSQ. When available, requests may be submitted via e-QIP. Investigative forms, releases, and fingerprint cards are to be mailed to:

Office of Personnel Management  
Federal Investigations Processing Center  
P.O. Box 700  
1137 Branchton Road  
Boyers, PA 16018-0700

Instructions for completing and submitting investigative requests are published in a guide entitled, "Requesting OPM Personnel Investigations," which can be obtained on-line from OPM Investigations Services (IS) site at [www.opm.gov/extra/investigate](http://www.opm.gov/extra/investigate). You will not be able to gain access to the IS site through the official OPM site.

AP2.4.1. The official submitting the request for investigation shall be responsible for ensuring that all documentation is completed in accordance with the instructions of the investigative provider.

AP2.5.1. The investigative provider shall establish procedures for requesting prior investigations, additional investigations to resolve derogatory or adverse information, and to request post-adjudication investigations.

AP3. APPENDIX 3

DOD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES

AP3.1. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE PERSONNEL SECURITY CLEARANCES (TOP SECRET, SECRET, AND CONFIDENTIAL)

AP3.1.1. Secretary of Defense and/or single designee

AP3.1.2. Secretary of the Army and/or single designee <sup>1</sup>

AP3.1.3. Secretary of the Navy and/or single designee <sup>1</sup>

AP3.1.4. Secretary of the Air Force and/or single designee <sup>1</sup>

AP3.1.5. Chairman of the Joint Chiefs of Staff and/or single designee

AP3.1.6. Director, Washington Headquarters Services, and/or single designee <sup>2</sup>

AP3.1.7. Director, National Security Agency, and/or single designee <sup>1,3</sup>

AP3.1.8. Director, Defense Intelligence Agency, and/or single designee <sup>1</sup>

AP3.1.9. Deputy General Counsel, Legal Counsel, OGC, and/or single designee (for contractors under the National Industrial Security Program (NISP))

AP3.1.10. Director, Defense Security Service, and/or single designee (may grant security clearances only for contractor personnel under the NISP)

AP3.2. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE LAA

Officials listed in AP3.1., above, and the Commanders of the Combatant Commands, or their single designee (must be at general officer, flag rank or civilian equivalent).

---

<sup>1</sup> 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 (b)), and DCID 6/4 (reference (k)). The authority for making SCI access eligibility determinations may also be the same official making security clearance determinations.

<sup>2</sup> The Director, Washington Headquarters Services, is authorized to grant, deny or revoke security clearances for civilian employees and assignees of Defense Agencies to which such authority has not been specifically assigned by this Regulation or by the Secretary/Deputy Secretary of Defense.

<sup>3</sup> 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 (h)).

### AP3.3. OFFICIALS AUTHORIZED TO ISSUE INTERIM CLEARANCES<sup>4</sup>

AP3.3.1. Interim TOP SECRET clearances shall be issued by the officials listed in AP3.1. This authority may be further delegated as deemed necessary.

AP3.3.2. Interim SECRET and CONFIDENTIAL clearances shall be issued by the officials listed in AP3.1. This authority may be delegated to organizational commanders.

### AP3.4. OFFICIALS AUTHORIZED TO SUSPEND ACCESS

#### AP3.4.1. Security Clearances

##### AP3.4.1.1. Contractor Personnel

AP3.4.1.1.1. The Director, Security, OASD(C3I) and the Deputy General Counsel (Legal Counsel), Office of General Counsel, OSD are authorized to suspend an individual's clearance as well as access.

AP3.4.1.1.2. Organizational commanders having jurisdiction over the contract or contractor may only suspend an individual's access.

##### AP3.4.1.2. Military and/or Civilian Personnel

AP3.4.1.2.1. Head of the DoD Component or adjudicative authority are authorized to suspend an individual's clearance as well as access.

AP3.4.1.2.2. Organizational commanders or supervisors having jurisdiction over the individual may only suspend their access.

#### AP3.4.2. Sensitive Compartmented Information. Cognizant SOICs, or their designees.

### AP3.5. PERSONNEL SECURITY APPEALS BOARD (PSAB)

A three-member PSAB shall be formed under the auspices of the officials listed in AP3.1.2. through AP3.1.8. to render final determinations when an unfavorable personnel security determination is appealed under Chapter 9.

---

<sup>4</sup> Interim access to SCI may only be determined by the SOIC, or their designated representative, as identified in AP3.1.

AP4. APPENDIX 4FAIR CREDIT REPORTING ACT NOTICE AND CONSENT

(Text taken verbatim from the Federal Trade Commission website)

**A Summary of Your Rights Under the Fair Credit Reporting Act**

The federal Fair Credit Reporting Act (FCRA) is designed to promote accuracy, fairness, and privacy of information in the files of every “consumer reporting agency” (CRA). Most CRAs are credit bureaus that gather and sell information about you--such as if you pay your bills on time or have filed bankruptcy--to creditors, employers, landlords, and other businesses. You can find a complete text of the FCRA, 15 U.S.C.1681-1681u, at the Federal Trade Commission’s web site (<http://www.ftc.gov>). The FCRA gives you specific rights, as outlined below. You may have additional rights under state law. You may contact a state or local consumer protection agency or a state attorney general to learn those rights.

- **You must be told if information in your file has been used against you.** Anyone who uses information from a CRA to take action against you -- such as denying an application for credit, insurance, or employment -- must tell you, and give you the name, address, and phone number of the CRA that provided the consumer report.
- **You can find out what is in your file.** At your request, a CRA must give you the information in your file, and a list of everyone who has requested it recently. There is no charge for the report if a person has taken action against you because of information supplied by the CRA, if you request the report within 60 days of receiving notice of the action. You also are entitled to one free report every twelve months upon request if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you up to eight dollars.
- **You can dispute inaccurate information with the CRA.** If you tell a CRA that your file contains inaccurate information, the CRA must investigate the items (usually within 30 days) by presenting to its information source all relevant evidence you submit, unless your dispute is frivolous. The source must review your evidence and report its findings to the CRA. (The source also must advise national CRAs -- to which it has provided the data -- of any error.) The CRA must give you a written report of the investigation, and a copy of your report if the investigation results in any change. If the CRA’s investigation does not resolve the dispute, you may add a brief statement to your file. The CRA must normally include a summary of your statement in future reports. If an item is deleted or a dispute statement is filed, you may ask that anyone who has recently received your report be notified of the change.
- **Inaccurate information must be corrected or deleted.** A CRA must remove or correct inaccurate or unverified information from its files, usually within 30 days after you dispute it. However, the CRA is not required to remove accurate data from your file unless it is outdated (as described below) or cannot be verified. If your dispute results in any change to your report, the CRA cannot reinsert into your file a disputed item unless the information source verifies its accuracy and completeness. In addition, the CRA must give you a written notice telling you it has reinserted the item. The notice must include the name, address and phone number of the information source.

- **You can dispute inaccurate items with the source of the information.** If you tell anyone -- such as a creditor who reports to a CRA -- that you dispute an item, they may not then report the information to a CRA without including a notice of your dispute. In addition, once you've notified the source of the error in writing, it may not continue to report the information if it is, in fact, an error.
- **Outdated information may not be reported.** In most cases, a CRA may not report negative information that is more than seven years old; ten years for bankruptcies.
- **Access to your file is limited.** A CRA may provide information about you only to people with a need recognized by the FCRA -- usually to consider an application with a creditor, insurer, employer, landlord, or other business.
- **Your consent is required for reports that are provided to employers, or reports that contain medical information.** A CRA may not give out information about you to your employer, or prospective employer, without your written consent. A CRA may not report medical information about you to creditors, insurers, or employers without your permission.
- **You may choose to exclude your name from CRA lists for unsolicited credit and insurance offers.** Creditors and insurers may use file information as the basis for sending you unsolicited offers of credit or insurance. Such offers must include a toll-free phone number for you to call if you want your name and address removed from future lists. If you call, you must be kept off the lists for two years. If you request, complete, and return the CRA form provided for this purpose, you must be taken off the lists indefinitely.
- **You may seek damages from violators.** If a CRA, a user or (in some cases) a provider of CRA data, violates the FCRA, you may sue them in state or federal court.

**Fair Credit Reporting Act of 1970, as amended**

**PLEASE TAKE NOTICE THAT ONE OR MORE CONSUMER CREDIT REPORTS MAY BE OBTAINED FOR EMPLOYMENT PURPOSES PURSUANT TO THE FAIR CREDIT REPORTING ACT, AS AMENDED, 15 U.S.C. 1681, ET SEQ. SHOULD A DECISION TO TAKE ANY ADVERSE ACTION AGAINST YOU BE MADE, BASED EITHER IN WHOLE OR IN PART ON THE CONSUMER CREDIT REPORT, THE CONSUMER REPORTING AGENCY THAT PROVIDED THE REPORT PLAYED NO ROLE IN THE AGENCY DECISION TO TAKE SUCH ADVERSE ACTION.**

Information provided by you on this form will be furnished to the consumer reporting agency in order to obtain information in connection with an investigation to determine your (1) fitness for Federal employment, (2) clearance to perform contractual service for the Federal Government, and/or (3) security clearance or access. The information obtained may be redisclosed to other Federal agencies for the above purposes and in fulfillment of official responsibilities to the extent that such disclosure is permitted by law.

I hereby authorize the \_\_\_\_\_, to obtain such reports from any  
(Name of Requesting Agency)  
consumer/credit reporting agency for employment, contractual or security clearance or access purposes.

\_\_\_\_\_  
(Print Name)

\_\_\_\_\_  
\*(SSN)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

\* Your Social Security Number is needed to keep records accurate, because other people may have the same name. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

## AP5. APPENDIX 5

### ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

The content of this Appendix is taken verbatim from the Adjudicative Standards approved by the President in March 1997. The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, amended Title 10, United States Code, to add a new section that precludes the initial granting or renewal of a security clearance by the Department of Defense under specific circumstances. These provisions have been incorporated into Guidelines H (Drug Involvement), I (Emotional, Mental, and Personality Disorders), and J (Criminal Conduct). Italicized type denotes the added provisions for DoD.

#### A. INTRODUCTION

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 (SCI) and Special Access Programs (SAPs) and are to be used by government departments and agencies in all final clearance determinations.

#### B. ADJUDICATIVE PROCESS

1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- a. The nature, extent, and seriousness of the conduct;
- b. The circumstances surrounding the conduct, to include knowledgeable participation;
- c. The frequency and recency of the conduct;
- d. The individual's age and maturity at the time of the conduct;
- e. The voluntariness of participation;
- f. The presence or absence of rehabilitation and other pertinent behavioral changes;

- g. The motivation for the conduct;
- h. The potential for pressure, coercion, exploitation, or duress; and
- i. The likelihood of continuation or recurrence.

2. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

3. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

- a. Guideline A: Allegiance to the United States
- b. Guideline B: Foreign influence
- c. Guideline C: Foreign preference
- d. Guideline D: Sexual behavior
- e. Guideline E: Personal conduct
- f. Guideline F: Financial considerations
- g. Guideline G: Alcohol consumption
- h. Guideline H: Drug involvement
- i. Guideline I: Emotional, mental, and personality disorders
- j. Guideline J: Criminal conduct
- k. Guideline K: Security Violations
- l. Guideline L: Outside activities
- m. Guideline M: Misuse of Information Technology Systems

4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigation may be

terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

5. 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:

- a. Voluntarily reported the information
- b. Was truthful and complete in responding to questions
- c. Sought assistance and followed professional guidance, where appropriate
- d. Resolved or appears likely to favorably resolve the security concern
- e. Has demonstrated positive changes in behavior and employment
- f. Should have his or her access temporarily suspended pending final adjudication of the information.

6. 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.

## GUIDELINE A

### ALLEGIANCE TO THE UNITED STATES

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

*Conditions that could raise a security concern and may be disqualifying include:*

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

b. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

c. Association or sympathy with persons or organizations that advocate the overthrow of the U.S. Government, or any state or subdivision, by force or violence or by other unconstitutional means;

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

*Conditions that could mitigate security concerns include:*

a. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

b. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

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

d. The person has had no recent involvement or association with such activities.

## GUIDELINE B

### FOREIGN INFLUENCE

*The Concern:* A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

*Conditions that could raise a security concern and may be disqualifying include:*

- a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;
- b. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;
- c. Relatives, cohabitants, or associates who are connected with any foreign government;
- d. Failing to report, where required, associations with foreign nationals;
- e. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;
- f. Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;
- g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;
- h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

*Conditions that could mitigate security concerns include:*

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

- c. Contact and correspondence with foreign citizens are casual and infrequent;
- d. The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;
- e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

## GUIDELINE C

### FOREIGN PREFERENCE

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

*Conditions that could raise a security concern and may be disqualifying include:*

- a. The exercise of dual citizenship;
- b. Possession and/or use of a foreign passport;<sup>1</sup>
- c. Military service or a willingness to bear arms for a foreign country;
- d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;
- e. Residence in a foreign country to meet citizenship requirements;
- f. Using foreign citizenship to protect financial or business interests in another country.
- g. Seeking or holding political office in the foreign country;
- h. Voting in foreign elections; and
- i. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

*Conditions that could mitigate security concerns include:*

- a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;
- b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;
- c. Activity is sanctioned by the United States;
- d. Individual has expressed a willingness to renounce dual citizenship.

---

<sup>1</sup> DoD Policy: A clearance shall be denied or revoked unless the applicant surrenders the foreign passport or obtains official approval for its use from the appropriate agency of the United States Government. The Statement of Reasons must inform the applicant that surrendering the passport to the foreign country and providing proof of its return or proof that the passport has been destroyed can also mitigate possession of a foreign passport.

GUIDELINE D  
SEXUAL BEHAVIOR

*The Concern:* Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion.<sup>1</sup> 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:*

- a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
- b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;
- c. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;
- d. Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

*Conditions that could mitigate security concerns include:*

- a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;
- b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;
- c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;
- d. The behavior no longer serves as a basis for coercion, exploitation, or duress.

---

<sup>1</sup> The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.

## GUIDELINE E

### PERSONAL CONDUCT

*The Concern:* Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

- a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or
- b. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

*Conditions that could raise a security concern and may be disqualifying also include:*

- a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;
- b. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
- c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;
- d. Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;
- e. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;
- f. Association with persons involved in criminal activity.

*Conditions that could mitigate security concerns include:*

- a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;
- b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;
- c. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;
- d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;
- e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;
- f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements, and upon being made aware of the requirement, fully and truthfully provided the requested information;
- g. Association with persons involved in criminal activities has ceased.

## GUIDELINE F

### FINANCIAL CONSIDERATIONS

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

*Conditions that could raise a security concern and may be disqualifying include:*

- a. A history of not meeting financial obligations;
- b. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;
- c. Inability or unwillingness to satisfy debts;
- d. Unexplained affluence;
- e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

*Conditions that could mitigate security concerns include:*

- a. The behavior was not recent;
- b. It was an isolated incident;
- c. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);
- d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
- e. The affluence resulted from a legal source; and
- f. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

## GUIDELINE G

### ALCOHOL CONSUMPTION

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

*Conditions that could raise a security concern and may be disqualifying include:*

- a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;
- b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;
- c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;
- d. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;
- e. Habitual or binge consumption of alcohol to the point of impaired judgment;
- f. Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of a alcohol rehabilitation program.

*Conditions that could mitigate security concerns include:*

- a. The alcohol-related incidents do not indicate a pattern;
- b. The problem occurred a number of years ago and there is no indication of a recent problem;
- c. Positive changes in behavior supportive of sobriety;
- d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participated frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

## GUIDELINE H

### DRUG INVOLVEMENT

*The Concern:*

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

b. Drugs are defined as mood and behavior-altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) Inhalants and other similar substances.

c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

*Conditions that could raise a security concern and may be disqualifying include:*

a. Any drug abuse (see above definition);<sup>1</sup>

b. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

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

d. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

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

---

<sup>1</sup> Under the provisions of 10 U.S.C. 986 (reference (rr)), any person who is an unlawful user of, or is addicted to, a controlled substance as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802) (reference (ss)), may not be granted or have renewed their access to classified information.

*Conditions that could mitigate security concerns include:*

- a. The drug involvement was not recent;
- b. The drug involvement was an isolated or aberrational event;
- c. A demonstrated intent not to abuse any drugs in the future;
- d. Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

## GUIDELINE I

## EMOTIONAL, MENTAL, AND PERSONALITY DISORDERS

*The Concern:* Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

*Conditions that could raise a security concern and may be disqualifying include:*

- a. An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;<sup>1</sup>
- b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;
- c. A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;
- d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

*Conditions that could mitigate security concerns include:*

- a. There is no indication of a current problem;
- b. Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission, and has a low probability of recurrence or exacerbation;
- c. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

---

<sup>1</sup> Under the provisions of 10 U.S.C. 986 (reference (rr)), any person who is mentally incompetent, as determined by a credentialed mental health professional approved by the Department of Defense, may not be granted or have renewed their access to classified information.

## GUIDELINE J

### CRIMINAL CONDUCT

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

*Conditions that could raise a security concern and may be disqualifying include:*

- a. Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;
- b. A single serious crime or multiple lesser offenses.
- c. Conviction in a Federal or State court, including a court-martial of a crime and sentenced to imprisonment for a term exceeding one year;<sup>1</sup>
- d. Discharge or dismissal from the Armed Forces under dishonorable conditions;<sup>2</sup>

*Conditions that could mitigate security concerns include:*

- a. The criminal behavior was not recent;
- b. The crime was an isolated incident;
- c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;
- d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;
- e. Acquittal;
- f. There is clear evidence of successful rehabilitation.
- g. Potentially disqualifying conditions c. and d., above, may not be mitigated unless, where meritorious circumstances exist, the Secretary of Defense or the Secretary of the Military Department concerned has granted a waiver.

---

<sup>1</sup> Under the provisions of 10 U.S.C. 986 (reference (rr)) a person who has been convicted in a Federal or State court, including courts martial, and sentenced to imprisonment for a term exceeding one year, may not be granted or have renewed access to classified information. In a meritorious case, the Secretary of Defense or the Secretary of the Military Department concerned, may authorize a waiver of this prohibition.

<sup>2</sup> Under the above mentioned statute, a person who has received a dishonorable discharge or has been dismissed from the Armed Forces may not be granted or have renewed access to classified information. The same waiver provision also applies.

## GUIDELINE K

### SECURITY VIOLATIONS

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

*Conditions that could raise a security concern and may be disqualifying include:*

- a. Unauthorized disclosure of classified information;
- b. Violations that are deliberate or multiple or due to negligence.

*Conditions that could mitigate security concerns include actions that:*

- a. Were inadvertent;
- b. Were isolated or infrequent;
- c. Were due to improper or inadequate training;
- d. Demonstrate a positive attitude towards the discharge of security responsibilities.

## GUIDELINE L

### OUTSIDE ACTIVITIES

*The Concern:* Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

*Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:*

- a. A foreign country;
- b. Any foreign national;
- c. A representative of any foreign interest;
- d. Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

*Conditions that could mitigate security concerns include:*

- a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;
- b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

## GUIDELINE M

### MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

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

*Conditions that could raise a security concern and may be disqualifying include:*

- a. Illegal or unauthorized entry into any information technology system;
- b. Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;
- c. Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
- d. Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

*Conditions that could mitigate security concerns include:*

- a. The misuse was not recent or significant;
- b. The conduct was unintentional or inadvertent;
- c. The introduction or removal of media was authorized;
- d. The misuse was an isolated event;
- e. The misuse was followed by a prompt, good faith effort to correct the situation.

## AP6. APPENDIX 6

### POSITIONS REQUIRING ACCESS TO DoD INFORMATION TECHNOLOGY (IT) SYSTEMS AND NETWORKS

#### AP6.1. PURPOSE

This appendix establishes standard categories for positions within the Department of Defense and within defense contractor facilities that could be exploited by the individuals who are assigned to positions that directly or indirectly affect the operation of unclassified information technology (IT) resources and systems that process For Official Use Only (FOUO) and other controlled unclassified information. Such positions are referred to as IT and IT-related positions. These categories are to be used to distinguish and categorize the impact that individuals with certain IT privileges could have on DoD functions and operations.

The appendix also includes investigative and adjudicative requirements associated with these positions. The requirements of this appendix, are to be applied to all IT positions, whether occupied by DoD civilian employees, military personnel, consultants, contractor personnel or others affiliated with DoD (e.g., volunteers).

In today's environment, personnel in nearly every work situation use a computer to perform their assigned duties. In most of these situations, IT systems and resources are used as tools that enhance the incumbent's ability to accomplish their assignments. While these positions may require knowledge of various applications and skill in using available IT resources, the incumbents are not involved in developing, delivering, or supporting IT systems and services, or safeguarding sensitive data within such systems. Such IT users do not normally occupy IT positions and are not subject to the requirements of this Appendix. Their access, however, will be subject to established disclosure and security policies, such as described in section AP6.6.

#### AP6.2. DEFINITIONS

<b>Information Technology (IT)</b>	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
<b>Limited Privileged Access</b>	Privileged access with limited scope, e.g., an authority to change user access to data or system resources for a single information system (IS) or physically isolated network.
<b>Non-privileged Access</b>	User level access, i.e., normal access given to a typical user. Generally, all access to system resources is controlled in a way that does not permit those controls/rules to be changed or bypassed.

## **Controlled Unclassified Information**

Unclassified information that requires application of controls and protective measures for a variety of reasons. Examples of controlled unclassified information include, but are not limited to, the following categories:

- (1) For Office Use Only (FOUO): Information that may be withheld from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (ii)).
- (2) Unclassified Technical Data: Data related to critical technology with military or space application which may not be exported lawfully without approval, licenses or authorization under the Arms Export Control Act.
- (3) Department of State Sensitive But Unclassified (SBU): Information which originated from the Department of State (DoS) which has been determined to be SBU under appropriate DoS information security policies
- (4) Foreign Government Information: Information provided by a foreign government or governments, an international organization of governments or any element thereof, with the expectation that the information or source of the information, or both, are to be held in confidence.
- (5) Privacy Data: Personal and private information (e.g., individual medical information, home address and telephone number, social security number) as defined in the Privacy Act (reference (pp)).
- (6) Sensitive Information (Computer Security Act of 1987): Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act) (reference (pp)), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DoD payroll, finance, logistics, and personnel management systems.

## **Privileged Access**

Authorized access that provides capability to alter the properties, behavior or control of the information system/network. It includes, but is not limited to, any of the following types of access:

- (1) “Super user,” “root,” or equivalent access, such as access to the control functions of the information system/network, administration of user accounts, etc.

- (2) Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.
- (3) Ability and authority to control and change program files, and other users' access to data.
- (4) Direct access to operating system level functions (also called unmediated access) which would permit system controls to be bypassed or changed.
- (5) Access and authority for installing, configuring, monitoring or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations.

### AP6.3. GENERAL GUIDANCE

AP6.3.1. Defense in-depth requires, and DoD Directive 5200.28 (reference (tt)) specifies, that information systems/networks be safeguarded through use of a mixture of administrative, procedural, physical, communications, emanations, computer, and personnel security measures, that together achieve the requisite level of security. As DoD becomes increasingly dependent upon information technology to execute the DoD mission, ensuring the trustworthiness of all personnel, including temporary, seasonal, and intermittent employees, contractors, and volunteers, who have access to IT systems and networks is critical.

AP6.3.2. The type of access authorized (privileged, limited privilege, or non-privileged) is key to determining the level of trustworthiness required. It measures an incumbent's capability to effect the operation of DoD information systems and networks and potential to adversely impact the Department's overall security posture or ability to execute its mission.

AP6.3.3. The requirements of this appendix are intended to enhance the security of DoD IT systems and networks and to safeguard controlled unclassified information. In those cases where controlled unclassified information (e.g., critical technologies and Privacy Act data) is maintained in contractor owned and operated IT systems that have no interconnection (including data feeds) with DoD IT systems or networks, other safeguards (e.g., non-disclosure agreements, training) authorized in accordance with other applicable guidance may be used at the IT-III level in lieu of background investigations to mitigate the risks associated with the loss/misuse or unauthorized access to or modification of controlled unclassified information.

AP6.3.4. Level of access granted must be supported by the appropriate investigative basis/authority for holding a position at that level.

AP6.3.5. This policy applies to contractors and consultants who require access to DoD systems and networks and shall be implemented through incorporation in their contracts.

AP6.3.6. For cases in which the investigative requirements for IT access exceed the investigative requirements for access to classified information/security clearance requirements, the higher requirement must be met.

AP6.3.7. Users of this appendix are also cautioned that other policies may levy additional requirements that must be met prior to assignment to a particular position requiring IT access. For example, each Designated Approving Authority (DAA), Information System Security Managers (ISSM), and Information System Security Officer (ISSO) must be a U.S. citizen; DAAs additionally must be U.S. Government personnel. Similarly, Verifying Officials (VO) and personnel appointed to operate Certificate Management Authority (CMA) equipment in support of DoD Public Key Infrastructure (PKI) must be U.S. citizens. It is the user's responsibility to be aware of additional requirements pertinent to the specific IT environment and to factor those requirements into this process at the appropriate places.

AP6.3.8. A phased implementation plan beginning in FY03 will be issued via memorandum in order to provide DoD Components sufficient time to comply with the policy contained in this Appendix.

#### AP6.4. IT ACCESS CATEGORIES

This paragraph defines IT access categories based on level of information system/network access required to execute responsibilities of the position and the associated potential for adverse impact on the DoD mission. DoD components are responsible for designation of each position as requiring privileged, limited privilege, or non-privileged access. Positions may be categorized at the higher level as needed to account for ability to impact overall network/system security posture, intended system behavior, or appropriate content. DoD agencies that issue contracts requiring access to DoD IT systems/network shall provide specific guidance to their contractors regarding the categorization of contractor positions and the investigative requirements of this Regulation.

AP6.4.1. IT-I Position. Incumbent of this position has privileged access to networks and information systems, system security and network defense systems, or to system resources. Duties are broad in scope and authority and provide access to the U.S. Government, DoD, or Component mission critical systems. The potential exists for exceptionally serious adverse impact on U.S. Government, DoD, Component or private sector information and/or operations, with worldwide or government-wide effects. Incumbent may also be responsible for unsupervised funds disbursements or transfers or financial transactions totaling over \$10M per year.

AP6.4.2. IT-II Position. Incumbent of this position has limited privileged access, but duties are of considerable importance to the DoD or DoD Component mission, and the incumbent is under the supervision of an individual in a higher trust position (IT-I). For example, individuals in these positions may have ability to impact a limited set of explicitly defined privileged functions, such as privileged access confined to large portions of an IT or to a local network physically isolated from other DoD or publicly accessible networks. The potential exists for moderate to serious adverse impact on DoD or Component information or operations.

Incumbent may also be responsible for monitored/audited funds disbursements or transfers or financial transactions totaling less than \$10M per year.

AP6.4.3. IT-III Position. Incumbent in this position has non-privileged access to one or more DoD information systems/applications. IT-III incumbents can receive, enter and/or modify information in an information system/application or database to which they are authorized access. Users have access only to that data/information and those applications/networks to which the incumbent is explicitly authorized or has need-to-know and cannot alter those or other users' authorizations. Positive security measures and configuration management ensures that the incumbent can assume only explicitly authorized roles and privileges. The potential exists for limited adverse impact on DoD, Component or unit information or operations. Incumbent may also be responsible for financial operations subject to routine supervision or approval, but has no funds disbursement or transfer capabilities.

#### AP6.5. TYPICAL CATEGORY ASSIGNMENT BY IT SPECIALTY

AP6.5.1. DoD components are responsible for categorization of each IT position at the highest level required by the specific duties, risks, and safeguards in place after analysis of the position's aggregated privileges, scope and levels of independence. Positions may be categorized at higher or lower levels as needed to account for ability to impact overall network/system security posture, intended system behavior, or appropriate content. However, when level of privilege and other position characteristics appear to indicate differing levels of categorization, the higher categorization assignment should be used.

AP6.5.2. The following are typical category assignments for each IT specialty title defined in the OPM Position Classification Standard "Administrative Work in the Information Technology Group, GS-2200" (<http://www.opm.gov/FEDCLASS/gs2200a.pdf>). Other IT-related positions should be categorized based on the particular set of duties and responsibilities of the position and the scope, and level of privileges authorized.

- a. Policy and Planning (PLCYPLN) – IT-III (IT-II if responsible for information security/information assurance program or if individual also has privileged access)
- b. Security (INFOSEC) – IT-I (IT-II if primarily policy, planning or awareness focused)
- c. Systems Analysis (SYSANALYSIS) – IT-III (IT-II if responsible for information security/information assurance systems)
- d. Applications Software (APPSW) – IT-I, -II, or -III depending on specifics of application (IT-I if responsible for information security/information assurance applications)
- e. Operating Systems (OS) – IT-II (IT-I if incumbent acts independently, without oversight/review)
- f. Network Services (NETWORK) – IT-I or IT-II (depending on the scope of network--as defined by criticality of or impact on Department or Federal government mission,

geographic reach, and/or major or significant impact on other government agencies and/or the private sector--and level of privileges)

- g. Data Management (DATAMGT) – IT-III (IT-II if responsible for safeguarding sensitive data/information)
- h. Internet (INET) – IT-II (IT-I if privileged access to network functions)
- i. Systems Administration (SYSADMIN) – IT-I (IT-II if stand-alone system or if ability to compromise limited to system/network operation)
- j. Customer Support (CUSTSPT) – IT-III (IT-I if privileged access; or IT-II if ability to set/change user access privileges (scope and level sensitive))

Other activities or specialties that may have significant IT duties include the following:

- a. Computer Clerk and Assistant (GS-335) or Computer Operation (GS-332) – typically IT-III, but may be higher if there is access to system/network control functions.
- b. Telecommunications (GS-391) (e.g., computer network analysts; data communications) – use appropriate IT specialty in subparagraph AP6.5.2 above
- c. Computer engineer (GS-0854) – generally hardware focused; typically IT-III, but specific categorization depends on function and application of the specific hardware/component (e.g., chip/board design may be IT-I), degree of supervision/review by higher authority, etc.
- d. Computer Science (GS-1550) – categorization depends on specific duties/responsibilities; use appropriate IT specialty in subparagraph AP6.5.2 above where possible.
- e. Criminal Investigating (GS-1811) – Law enforcement activities associated with computer/network crime (e.g., forensic analysis; criminal investigation) – categorization depends upon required level of access (e.g., privileged/non-privileged).
- f. Miscellaneous Management and Program Analysis (GS-343) and other scientists, subject matter experts, and professionals — depends upon required level of access (e.g., privileged/nonprivileged).
- g. Technical editors and other subject matter experts who develop web pages, but whose primary expertise is not technical knowledge of Internet systems, services, and technologies – categorize under “Internet” IT specialty; if non-privileged access, may be assigned IT-III designation

- h. Miscellaneous IT specialists (As required by specifics of new technology/ evolving specialty area) – use appropriate IT specialty in subparagraph AP6.5.2 above where possible.
- i. Threat and vulnerability assessment (e.g., red-teams; penetration testing) - determined by the purpose and scope of the assessment objective and required level of access.
- j. Certificate Management Authorities (CMA) to include Verifying Officials (VO) - typically IT-II, but may be higher if operating CMA equipment associated with Public Key Infrastructure operating above the DoD Class 4 assurance level.

#### AP6.6. ACCESS BY NON-U.S. CITIZENS

AP6.6.1. Access to unclassified information by a non-U.S. citizen shall only be permitted in accordance with applicable disclosure policies (e.g. DoD Directive 5230.9 (reference (uu)), DoD Directive 5230.25 (reference (vv)), DoD 5400.7-R (reference (ii)) and U.S. statutes (e.g., Arms Export Control Act). A non-U.S. citizen shall not be assigned to a DoD IT position requiring access to information that is not authorized for disclosure by the U.S. organization that originated the information to his or her country of citizenship.

AP6.6.2. Non-U.S. citizens assigned into DoD IT positions are subject to the investigative requirements outlined in section AP6.7. For non-U.S. citizens employed outside of the United States in countries hosting U.S. forces, investigative requirements are outlined in subparagraph C3.5.4.

AP6.6.2.1. A non-U.S. citizen may be assigned to an IT-I position if the head of the DoD Component or Agency that owns the system/information/network approves the assignment in writing. The written approval must be on file before requesting the required investigation. The required investigation must be completed and favorably adjudicated prior to authorizing IT-I access to DoD systems/networks. Interim access is not authorized. Every effort shall be made to minimize, and where possible eliminate, the number of non-U.S. citizens employed in IT-I positions. However, compelling reasons may exist to grant such access in those circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable U.S. citizen is not available.

AP6.6.2.2. Non-U.S. citizens may hold/be authorized access to IT-II and IT-III. The required investigation must be completed and favorably adjudicated prior to authorizing IT-II and IT-III access to DoD systems/networks. Interim access is not authorized.

AP6.6.3. By December 1 following the end of each fiscal year, the DoD Components will provide a report to the DASD(S&IO), OASD(C3I), containing the following data:

AP6.6.3.1. Number of non-U.S. citizens occupying a IT-I position, broken out by location, i.e., CONUS or OCONUS;

AP6.6.3.2. For each location (CONUS or OCONUS), the number of individuals by nationality.

#### AP6.7. LEVEL OF BACKGROUND INVESTIGATION

The required investigations for all IT-I, IT-II and IT-III positions are outlined below.

<b>Position Category</b>	<b>Civilian</b>	<b>Military</b>	<b>Contractor</b>	<b>Non-U.S. Citizen*</b>
IT-I	SSBI	SSBI	SSBI	SSBI, if approval granted
IT-II	NACI	NACLC	NACLC	NACLC
IT-III	NACI	NAC	NAC	NAC

\*Investigative requirements for non-U.S. citizens outside the U.S. are outlined in subparagraph C3.5.4.

Assignment (including assignments due to accretion of duties) of current DoD employees, military personnel, consultants and contractors to positions with increased access privileges requires verification of the appropriate investigative basis/authority for holding a position of that level of sensitivity.

#### AP6.8. REQUESTS FOR INVESTIGATION

AP6.8.1. IT investigations are to be submitted to OPM using the SF86. The form is to be completed only after a conditional offer of employment.

AP6.8.2. Each requester will need to establish a submitting office number (SON) with OPM before requesting an investigation. Appendix 2 contains guidance on submitting investigations to OPM. Your office must place this SON code on each request submitted to OPM.

AP6.8.3. Completed investigations are to be returned to OPM for a trustworthiness determination. To ensure the completed investigation is properly returned to OPM, the designation - OM25 - must be reflected in Item L when completing the Agency Use Block section.

AP6.8.4. When completing Item N, contractor requesters must indicate the appropriate billing code of the DoD contracting activity.

AP6.8.5. For cases in which the investigative requirements for IT access exceed the investigative requirements for access to classified information; the higher requirement must be met.

#### AP6.9. INTERIM ASSIGNMENT

AP6.9.1. Individuals, except non-U.S. citizens, to include temporary, intermittent and seasonal personnel, may be assigned to IT-I, IT-II, or IT-III positions on an interim basis prior to

a favorable adjudication of the required personnel security investigation only after the conditions specified below have been met. Interim access is not authorized for non-U.S. citizens.

AP6.9.1.1. IT-I:

AP6.9.1.1.1. Favorable completion of the NAC (current within 180 days)

AP6.9.1.1.2. Initiation of an SSBI/favorable review of SF86

AP6.9.1.2 IT-II:

AP6.9.1.2.1. A favorable review of local personnel, base/military, medical, and other security records as appropriate

AP6.9.1.2.2. Initiation of a NACI (for civilians) or NACLC (for military and contractors), as appropriate/favorable review of SF86

AP6.9.1.3. IT-III:

AP6.9.1.3.1. A favorable review of local personnel, base/military, medical, and other security records as appropriate

AP6.9.1.3.2. Initiation of a NACI (for civilians) or NAC (for military and contractors), as appropriate/favorable review of SF86

AP6.9.2. For DoD civilian and military personnel, the approval for interim assignment shall be made by the security manager at the requesting activity. For DoD contractor personnel, approval authority for interim assignment reside with the government sponsor's security manager/official, but may be delegated to the contractor's senior security official with the approval of the Head of the DoD Component or Agency that owns the system/information.

AP6.10. ADJUDICATION

AP6.10.1. Completed investigations will be forwarded to OPM (SOI: OM25) for a trustworthiness determination. Adverse cases will be sent to DOHA for final action. The submitting entity will be notified in writing regarding the results of the OPM/DOHA decision. The guidelines in Appendix 5 and procedures in Chapter 9 will serve as the basis for most decisions. In certain cases, status as a non-U.S. citizen is not an automatic disqualifier. For contractor personnel, trustworthiness determinations are outside the provisions of the NISP.

AP6.10.2. All trustworthiness determinations will be entered into JPAS.

AP6.11. REINVESTIGATION

Individuals occupying a position requiring IT access shall be subject to an aperiodic reinvestigation under the forthcoming ACES (estimate June 2003).

### AP6.12. PRIOR BACKGROUND INVESTIGATIONS

If an individual previously has been subject to background investigative and adjudicative requirements, depending on the age of the investigation those requirements may not need to be duplicated for IT access. Investigative criteria for DoD personnel and contractors/consultants who have had prior background investigations are outlined in the table below.

IT Position Category/Investigative Equivalency Table  
DoD Civilian and Military Personnel, Contractors, and Consultants

<i>If Position Category is:</i>	<i>Individual has/had the following investigation:</i>	<i>And the age of the investigation is:</i>	<i>Then the investigation required is:</i>
<b>IT-I</b>	SSBI	< 5 yrs	None
	SSBI-PR	> 5 yrs	SSBI-PR
	SBI BI LBI MBI NACL ANACI NAC NACIC ENTNAC	Regardless of age of the investigation	SSBI
<b>IT-II</b>	SSBI SSBI-PR	< 10 yrs	None
	SBI BI LBI MBI NACL ANACI NACIC	> 10 yrs	NACL
	ENTNAC NAC	Regardless of age of the investigation	NACL (contractor, military) NACI (civilian)
<b>IT-III</b>	SSBI SBI	< 15 yrs	None
	BI SSBI-PR LBI MBI ANACI NACL NAC NACIC ENTNAC	> 15 yrs	NAC (contractor, military) NACI (civilian)

### AP6.13. TRAINING AND AWARENESS REQUIREMENTS

DoD Components must ensure that individuals with access to DoD IT systems and networks receive the requisite information assurance, security awareness, and functional competency training as required by their designated level of access and scope of duties, and that the training is documented in individual personnel files. Understanding the threats, system vulnerabilities, and protective measures required to counter such threats are key features to a core information assurance awareness program at each IT access level.

AP7. APPENDIX 7

**LIST OF SAMPLE NOTIFICATIONS**

	<u>Page</u>
<b>Initial Package to Notify Organization and Individual</b>	
Local Organization Letter with SOR .....	133
Sample SOR (Enclosure 1 to Letter) .....	135
Security Concerns and Supporting Adverse Information .....	136
Instructions for Responding to SOR .....	137
Sample Applicable Personnel Security Guidelines (Enclosure 2 to Letter) .....	140
SOR Receipt and Statement of Intention (Enclosure 3 to Letter).....	141
Request for Access to Personal Records.....	142
<b>Package to Inform Organization and Individual of Denial</b>	
Local Organization Letter with LOD.....	143
Sample Letter of Denial (Enclosure to Letter).....	145
Notice of Intent to Appeal.....	147
Instructions for Appealing a Letter of Denial/Revocation (LOD).....	148

**Local Organization Letter with Statement of Reasons (SOR)**

From: Director, (Component) Central Adjudication Facility  
To: Director, Service Graphics Facility, Washington, D.C.  
Subject: Responsibility for Handling Statement of Reasons (SOR)  
Reference: (a) DoD 5200.2-R

Enclosures: 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 person named in the enclosed SOR. Since denial or revocation of access eligibility can have a severe impact on employees 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 person named in the SOR:

a. Consider whether or not to suspend access to classified information and assignment of the subject 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 subparagraph C9.2.2.1., of Chapter 9 of the reference. This person will serve as a liaison between the (Component) Central Adjudication Facility (CAF) and the subject.

3. The POC from your organization should:

a. Promptly deliver enclosure (1) to this letter, the SOR and its enclosures, to the subject.

b. Ensure completion of enclosure (2) to this letter and forward it to the CAF within ten calendar days. Ensure that Parts I, II, and III are all completed. This form notifies the CAF whether the subject intends to respond to the SOR and whether your organization has granted a time extension.

c. Advise the subject 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 subject understands that he or she is entitled to obtain legal counsel or other assistance but that this must be done at his or her own expense.

d. Ensure that the subject 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 subject fully understands that the proposed denial or revocation action will become final if your organization notifies the CAF via enclosure (2) that the subject does not intend to respond to the SOR. Ensure that the subject 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 subject 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 subject in obtaining applicable references and copies of pertinent investigative files. The SOR is usually based on investigative information from the Defense Security Service (DSS) and/or another investigative agency. If the subject 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 subject wants to obtain a copy of the complete investigative file, provide him or her with enclosure (3) which is the form for requesting DSS and/or other investigative agency records under the Privacy Act (5 U.S.C. 552a.). Send requests to: Defense Security Service Privacy Act Branch, 601 10<sup>th</sup> Street, Suite 128, Fort Meade, MD 20755-5134.

4. Ensure that the subject'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](mailto:doejohn@caf.dod).

### Statement of Reasons (SOR)

From: Director, (Component) Central Adjudication Facility

Through: Director, Service Graphics Facility, Washington, D.C.

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

Enclosures: 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, or 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 ten 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 1995 in Arlington, Virginia, for assault on a police officer. You were found guilty and fined \$4,000.
  - b. You were arrested on 10 January 1993 in Fairfax, Virginia, 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 1993 in Fairfax, Virginia, 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, D.C. 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, D.C. 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, D.C., was \$350 overdue and referred for collection.
  - d. As of 20 July 1994, your credit account with J. C. Penney Co., Arlington, Virginia, 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 ten 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 ten 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 letters 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 and III 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 extension for the following reason(s):

\_\_\_\_\_  
 \_\_\_\_\_

- c.  respond via my organization head within 30 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.

Point of Contact: \_\_\_\_\_  
 (Printed Name) (Signature) (Telephone No.)

<b>REQUEST FOR ACCESS TO PERSONAL RECORDS</b>				
SUBMIT TO: DEFENSE SECURITY SERVICE, PRIVACY ACT BRANCH, 801 10 <sup>TH</sup> STREET, SUITE 128, FORT MEADE, MD 20755-5134				
<b>SECTION I - PRIVACY ACT ADVISEMENT</b>				
Requesting personal information concerning you, including your Social Security Number (SSN), is authorized by 5 USC 552a. Providing all or part of this information is voluntary. However, without it the Defense Security Service (DSS) may not be able to identify records. The information provided herein will be used to identify and retrieve records pertaining to the individual identified in the request and to protect the privacy of individuals on whom DSS maintains records. This information will be retained in the files of DSS and may be released to other components or agencies for official purposes.				
<b>SECTION II - RECORD IDENTIFICATION AND REQUEST FOR ACTION (Please Print or Type)</b>				
1a. Title: Mr. _____ Ms. _____ Other _____	1b. Last Name	1c. First Name	1d. Middle Name	1e. Suffix
2. Other names used (in Last, First, Middle format)			3. Social Security Number (SSN)	
			4. Date of Birth (in MM/DD/YY format)	
8. Your current mailing address			5. Place of Birth (including Country, if not USA)	
			6. Home phone number (Include Area Code)	
			7. Work phone number (Include Area Code)	
9. Description of records sought (Investigative File, etc.) and information which may assist in locating information (DOD affiliation, dates of invest., etc.)				
10. Check here if you wish: _____ a. a copy of your records. _____ b. the identity of activities to which your records were disclosed. _____ c. to be informed if DSS is aware of other agencies maintaining records concerning you. _____ d. Other (Specify) _____			11. If you wish your records sent to another person or agency, provide the name, address and phone number here:	
12. CERTIFICATION I certify that the above information is correct and that I am the person described in blocks 1 through 8.			SIGNATURE:	
<b>SECTION III - NOTARY CERTIFICATION OF REQUESTER IDENTIFICATION</b> False Statements Subject to Criminal Penalties. See Public Law 93-579, 88 Stat 1902 (USC 552a(1))				
I, _____ a Notary Public in and for the County (City) and State of _____				
hereby certify that on the _____ day of _____, _____, before me personally appeared _____ who is known by me to be the identical person whose name is subscribed to, and who signed and executed the foregoing instrument in witness whereof, I have hereunto set my hand and official seal this day and year above.				
My commission expires _____ Notary Public _____				
<b>SECTION IV - AGENCY RECEIPT</b>				
DATE RECEIVED AT DSS/PAB	IDENTITY VERIFIED AT DSS/PAB	DSS/PAB CONTROL NUMBER		

### **Local Organization Letter with LOD**

**From:** Director, (Component) Central Adjudication Facility

**To:** Director, Service Graphic Facility, Washington, D.C.

**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 ten 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 prior to referral to the PSAB. If the individual desires a personal appearance, the request must be in writing. It must be sent to DOHA within ten 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 PSAB or Director, DOHA at DSN 226-4598 or commercial 703-696-4598 Extension 124, or by E-Mail.

### 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)

References: a. Our letter (Ser XXX of (date))  
b. Personnel Security Regulation  
c. Your letter of (date)

Enclosures: 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 1995. 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 ten 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), P.O. Box 3656, Arlington, Virginia 22203 (FAX No. 703-696-6865) within ten calendar days of your receipt of the LOD. A format (enclosure 1) for

requesting a personal appearance is provided on page 151. 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 the POC designated by your organization.

Use the following if the individual did not respond to the 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**

(COMPLETE ONLY IF YOU ARE GOING TO APPEAL)

**Part I**

I, (Name – Last, First, Middle – Filled in by CAF at LON issuance), (Rank or Grade), social security number (Filled in by CAF at LON issuance), received the (Name of CAF) final security determination on (Date to be filled in by appellant). I elect (check only one of the following):

to appeal directly to the Personnel Security Appeal Board (PSAB)

a personal appearance before a DOHA Administrative Judge

**Part II**

My contact information:

a. Duty Address (Complete Address)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. Duty Phone:

Commercial: \_\_\_\_\_

DSN: \_\_\_\_\_

FAX: \_\_\_\_\_

c. Home Address:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

d. Home Phone:

Commercial: \_\_\_\_\_

e. E-Mail Address:

Office: \_\_\_\_\_

Home (Optional): \_\_\_\_\_

f. My Security Manager, SSO or POC is:

Name: \_\_\_\_\_

Phone:

Commercial: \_\_\_\_\_

Address: \_\_\_\_\_

DSN: \_\_\_\_\_

E-Mail Address: \_\_\_\_\_

FAX: \_\_\_\_\_

**Part III**

a. If you elected to appeal directly to the PSAB, this Notice must be sent to: PSAB, PSAB address, within 10 calendar days from receipt of the Letter of Denial/Revocation.

b. If you elected a personal appearance, this notice must be sent or faxed to the appropriate CAF within 10 calendar days from receipt of the Letter of Denial/Revocation. Upon receipt of this Notice by the CAF, your case file and this Notice will be forwarded to DOHA.

\_\_\_\_\_  
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 you 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 ten calendar days of receipt of the LOD. You will receive a notice designating the time, date and place for the personal appearance, which generally will 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 areas.

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 may have the opportunity to present or cross-examine witnesses if the Director, DOHA or designee determines that testimony is needed to resolve a disputed material fact.

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 AJ will submit a transcript of your personal appearance to the PSAB. The PSAB will consider the recommendation of the AJ and render a decision regarding your eligibility.

## AP8. APPENDIX 8

### PERSONNEL SECURITY APPEAL BOARD (PSAB)

#### AP8.1. STRUCTURE AND FUNCTIONING OF THE PSAB

Component PSABs shall be structured and function to meet the following requirements:

AP8.1.1. 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 military grade of O-5 or civilian grade of GM/GS-14, at least one member of the board will be equivalent or senior in grade to the appellant.

AP8.1.2. 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.

AP8.1.3. 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.

AP8.1.4. 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.

AP8.1.5. Officials from the component CAF will neither serve as a member of the board nor communicate with board members concerning the merits of an open case.

AP8.1.6. Component PSABs will meet regularly to assure timely disposition of appeals.

AP8.1.7. 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.

AP8.1.8. Component PSABs will render a final determination and notify the subject (via the subject's local organization) in writing. The subject will generally be notified by the PSAB 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 CAF. The PSAB determination will be final and will conclude the appeal process.

AP8.1.9. The PSAB shall maintain a redacted file of all decisions, which will be subject to review in accordance with the Freedom of Information Act.

## AP9. APPENDIX 9

### INVESTIGATIVE PRIORITIES

#### AP9.1. GENERAL

AP9.1.1. Investigative priorities fall into nine categories and apply to both initial and periodic reinvestigations.

AP9.1.2. Requesters must be judicious in assigning priorities, ensuring use only when access cannot be granted or continued without completion of the investigation.

AP9.1.3. DoD Components shall ensure compliance by requesters with all appropriate prioritization requirements and ensure priority treatment of cases by the CAF.

AP9.1.4. Priority cases submitted to DSS must contain the two-position code (EPSQ 2.2) and will be conducted within specified timelines. The cases are to be completed on or before the number of days indicated. Investigations with leads pending overseas or at another agency may prevent timely completion of these priority cases.

AP9.1.4.1. NACLC – 75 days; NACLC-PR – 120 days

AP9.1.4.2. SSBI – 90 days; SSBI-PR – 120 days.

AP9.1.4.3. SII – 90 days

Investigations requiring faster completion times than the priority case timelines must be approved on a case-by-case basis.

AP9.1.5. Priority cases submitted to OPM must indicate service level needed i.e., 35-day service, 75-day service, or 120-day service. There is an increased cost for 35-day service.

#### AP9.2. PRIORITY INVESTIGATIONS AND CODES

Priority Codes	Type of Priority Investigation
11	Presidential Support (Yankee White)
12	Sensitive Compartmented Information (SCI)
13	Special Access Programs (SAPs)
14	Presidential Transition
15	Personnel Reliability Programs (PRP)
23	State Department investigations for contractor personnel employed in the construction of U.S. embassies
25	Contractors being deployed to support contingency or wartime operations, for example, contract linguists, who possess a critical skill in support of a DoD contingency mission.
26	Single Integrated Operational Plan – Extremely Sensitive Information (SIOP-ESI)
27	NATO/SHAPE commands/organizations

AP10. APPENDIX 10

PERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE (AJ)

AP10.1.1. A person appealing a Letter of Denial (LOD) may request a personal appearance by notifying DOHA in writing at the following address: Director, Defense Office of Hearings and Appeals, P.O. Box 3656, Arlington, VA 22203 (FAX No. 1-703-696-6865). The request must be sent to DOHA within ten 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.

AP10.1.2. Upon receipt of a request for a personal appearance, DOHA shall promptly 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 ten calendar days.

AP10.1.3. 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, D.C. metropolitan area or the Los Angeles, California metropolitan area as determined by the Director, DOHA, or designee.

AP10.1.4. Travel costs for the appellant will be the responsibility of the employing organization.

AP10.1.5. The AJ will conduct the personal appearance proceeding in a fair and orderly manner:

AP10.1.5.1. The appellant may be represented by counsel or personal representative at his and her own expense.

AP10.1.5.2. 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;

AP10.1.5.3. The appellant may submit documents relative to whether the LOD should be overturned;

AP10.1.5.4. The appellant may have the opportunity to present or cross-examine witnesses only upon a determination by the Director, DOHA, or designee, that the testimony is needed to resolve a disputed material fact, and that the witness will appear, at no expense to the Government except when requested to appear by DOHA Department Counsel, without undue delay of the proceeding;

AP10.1.5.5. Upon completion of the personal appearance, the AJ will 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;

AP10.1.6. The PSAB will render a final written determination stating its rationale and notify the individual in writing (via the individual's employing organization) within 30 calendar days of receipt of the recommendation from DOHA. This decision will be final and will conclude the appeal process.

AP11. APPENDIX 11PEER REVIEWAP11.1. GENERAL PROCEDURES

AP11.1.1. The review will consist of three components: a data call, site visit and report by a review team. Three reviews are to be conducted each fiscal year<sup>1</sup>. The data call will encompass all phases of CAF operations: organizational structure, budget, staffing, procedures, performance metrics, training, etc. The data call will change from time to time to reflect changes in adjudicative program requirements.

AP11.1.2. A suggested 3-year schedule for CAF reviews and team members is shown below. Composition of the teams may be rotated periodically.

Schedule of CAF Reviews and Team Membership<sup>2</sup>

		CAF providing team members								
	CAF Review	Army	Navy	AF	WHS	NSA	DIA	DISCO	DOHA	JCS
Year 1	Army	-	X		X		X	X		
	WHS	X		X	-				X	X
	DISCO		X					-	X	X
Year 2	Navy		-	X	X	X	X			
	NSA	X		X		-	X		X	
	DOHA		X		X			X	-	
Year 3	AF	X		-	X	X	X			
	DIA	X		X		X	-			X
	JCS		X					X		-

AP11.1.3. CAFs shall review their operations on a continuing basis and shall conduct a self-inspection midway between team reviews. As a minimum, self-inspections shall include all elements normally contained in team reviews. The CAF shall maintain a record of the self-inspection and the date it was accomplished. This record must be available for review during the next scheduled team review. Deficiencies identified during self-inspection shall be corrected as expeditiously as possible.

<sup>1</sup> Peer reviews will begin in CY03.

<sup>2</sup> Scheduling criteria: The CAF under review does not provide a team member.

## AP11.2. DATA CALL

**I. Cost Effectiveness/Resources.** The primary focus is to ascertain if the CAF has sufficient resources to perform its mission. The interest is on organizational structure, budget, and staffing.

- What is the CAF's Organizational Structure?
  - Reporting chain
  - Policy chain
  - Source(s) of operating funds
- Does the CAF have sufficient resources?
  - Staffing
    - Senior leadership/management
    - Adjudicators
    - Support personnel
    - Turnover
    - New Hires
  - Computers/Automation
  - Training

**II. Efficiency.** The primary interest is the production of the CAF and the automation available to assist the CAF to meet its mission.

- What is the workload of the CAF?
  - Cases per year by
    - Clearance type (S, TS, SCI)
    - Type Person cleared (military, civilian, industry)
    - Clean, minor issue, major issue, SOR, compelling need, due process, waiver
    - Component specific requirements
- What type of automation support does the CAF have?
  - Number computer terminals
  - Number JPAS terminals
  - New initiatives

**III. Operational Procedures.** The focus is on CAF procedures and metrics that measure CAF performance.

- By type of case (i.e. clean, issue, Secret, TS/SCI, PR, and Component specific requirements) what is the average length of time
  - to open cases
  - to adjudicate
  - to make JPAS entry
  - to notify recipient

- What are the CAF operating procedures for
  - promulgating guidance for adjudicative issues
  - opening cases
  - reviewing
    - for completeness of investigation
    - for issue/non-issue
  - adjudicating clean/issue cases?
  - issuing clearance for issue/non-issue
  - issuing SOR
  - granting waivers
  - due process cases
  - entry into JPAS
  - recording name of adjudicator(s) responsible for determination
  - recording adjudicator notes for determination
- What are the CAF metrics for performance ratings (successful, fully successful, exceptional)
  - for clean, minor issue, major issue, SOR, compelling need, waivers, due process
  - adjudicator grade level
- What are the metrics for overall CAF performance?
- What are the Component requirements for determinations for non-security personnel?
  - Requirements
  - Issued by
  - Time expended on these determinations
  - Grade level responsible for these determinations

**IV. Standardization.** This area address CAF procedures to ensure that determinations are consistent with standards.

- What is the training plan for the CAF?
  - Training provided by
    - in-house, DSS, Intel Community
    - Initial and continuing education
    - CAF comments on community training
  - Training content
    - Adjudicative guidelines
    - CI training
    - Component specific issues
- How many people were trained in past year? Grade level?
- What kinds of outside experts used by CAF?
  - Availability of medical, legal, financial, IT, psychological, polygraph, CI experts
  - in-house, Intel Community, other sources

- Number of times experts consulted in past year (medical, legal, financial, IT, CI, psychological, polygraph, etc)

- What procedures are used to assess and maintain CAF quality?
  - Case review by supervisors
  - Multiple review of cases
  - An adjudicator record of the number of cases adjudicated – clean/issue
  - A case record of which adjudicators worked on a case – clean/issue
  - Other
  
- Are cases available for inspection in terms of application of guidelines?
  - Recent
  - Non-issue and issue
  - Waivers
  - Compelling need
  
- Is a written record of adjudicative action and determination of a case available?
  - Mitigations

**V. Individual Rights vs. National Security.** This addresses CAF procedures for denying or revoking eligibility.

- What are the due process procedures?
  - Track length of time from opening to issuing SOR
  - Provide a copy of case material to Subject
  - Notify PSAB that case is in process
  - “Suspense” or track responses
    - from Subject
    - from PSAB
    - from personal appearance
  - Make entry to JPAS after final determination

INDEX

<b>A</b>		<b>I</b>	
Access		Interims	
Administrative withdrawal .....	61	Clearance .....	<i>See Security Clearance</i>
At a higher level .....	40	Information Technology .....	<i>See IT</i>
By retired individuals .....	41	Who can issue.....	99
Downgrade .....	63	Investigation	
Granting.....	59, 60, 75, 77	By other agencies.....	53
Adjudication		Non-U.S. citizen	
Function.....	56	IT <i>See IT</i>	
Process.....	64, 103	LAA .....	<i>See LAA</i>
Standards .....	103	Overseas .....	44
Support services.....	57	Overseas .....	26
Adverse Information		Prior .....	52
Resolving.....	22, 62	Priorities .....	151
Appeal		Requesting .....	54, 96
Clearance Decision .....	65	Requirements .....	93
How to .....	148	Standards .....	82
<b>B</b>		Timelines .....	17
Briefings		Trustworthiness .....	42
Initial .....	68	Investigative Records	
Refresher.....	69	Access.....	70
Termination .....	69	Disposition.....	72
Travel.....	69	Safeguarding.....	71
<b>C</b>		IT	
CNDWI .....	49	Interims.....	129
Consultants .....	38	Investigation requirement .....	129
Continuing Evaluation .....	67	IT Positions.....	126
Contract Linguists.....	50	Non-U.S. citizens.....	128
Contractors		Position Categories .....	125
Adjudication .....	15. <i>See Adjudication</i>	<b>J</b>	
Clearance .....	<i>See Security Clearance</i>	JPAS	
Investigation .....	<i>See Investigation</i>	Access.....	77
<b>D</b>		<b>L</b>	
DCH		LAA.....	<i>See Limited Access Authorization</i>
Access.....	73	Limited Access Authorization	
Definitions .....	8	Access.....	35
Due Process .....	<i>See Adjudication Process</i>	Limitations.....	35
<b>E</b>		Requirements.....	36
EOD.....	49	<b>M</b>	
<b>F</b>		Military Service	
Fair Credit Reporting Act (FCRA)		Investigative requirements.....	33
Consent .....	100	<b>N</b>	
Notice .....	100	NATO .....	49
Requirements .....	22	Non-U.S. citizen	
Foreign National .....	<i>See Non-U.S. citizen</i>	Clearance .....	<i>See LAA</i>
		Investigation .....	<i>See Investigation</i>

**O**Overseas Investigation..... *See* Investigation**P**

## Peer Review

Data Call.....155

Procedures .....80

Schedule .....154

## Periodic Reinvestigation (PR)

Requirements .....93

Personal Appearance .....149, 152

Personnel Security Appeal Board.....65, 150

## Personnel Security Investigations

Scope .....21

Standards ..... *See* Investigation

Type.....21

Presidential Support.....49

Prior Adjudications.....*See* ReciprocityPrior Investigations.....*See* Investigations

PRP.....49

**R**

## Reciprocity

Adjudications.....52, 53

Investigations.....53

Red Cross/USO .....43

**S**

SCI.....46

## Security Clearance

Interims.....34, 94

Investigative requirements.....34

Issuing .....59, 98

Non-U.S. citizen *See* LAA .....35

Previously granted .....35

Reapplication after Denial or Revocation.....65

## Sensitive Positions.....30

Critical-sensitive .....30

Investigative requirements.....31

Noncritical-sensitive.....31

## SIOP-ESI .....49

## Suspension

Actions.....62

Who can suspend .....99

**T**

Telephone Interviews .....28

Temporary Eligibility ..... *See* Interims

## Timelines

Adjudication .....17

Investigation .....17

Trustworthiness Determinations.....42

**W**

## Waiver

Investigative Requirements .....45

Smith Amendment .....103, 118