Army Regulation 380–67

Security

Personnel Security Program

Headquarters
Department of the Army
Washington, DC
9 September 1988

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–67
Personnel Security Program

This revision--

- Changes the number of the regulation from the 604-series to the 380-series.
- Expands the list of definitions and provides a list of acronyms (1-300 glossary).
- Requires reporting of information on individuals who have had access to sensitive compartmented information or other sensitive programs and who are being involuntarily separated from military service (2-201.2).
- Adds a requirement for a DOD National Agency Check and written inquiries for military and contractor personnel for access to SECRET information (2-303).
- Establishes a billet control system for all military and civilian positions requiring access to TOP SECRET information (3-104).
- Specifies that only U.S. citizens are eligible for security clearances (3-403).
- Provides guidance for access by persons outside the executive branch (3-404).
- Contains policy and procedures for personnel occupying ADP positions (3-614 and app K).
- Defines sensitively and categories of critical military duties (3-703.1).
- Clarifies due process procedures in unfavorable administrative action procedures (8-103 through 8-201.1).
- Establishes procedures for reporting personal foreign travel by persons with security clearances (9-203).
- Includes additional adjudication policy guidelines categories--Loyalty, Foreign Preference, Foreign Connections, Falsification, and Refusal to Answer (app I).
- Establishes procedures for Army military intelligence units to follow when conducting personnel security investigations for Defense Investigative Service overseas (app J).
- Provides an index to the regulation.

Headquarters
Department of the Army
Washington, DC
9 September 1988

*Army Regulation 380–67

Effective 7 October 1988

Security

Personnel Security Program

By Order of the Secretary of the Army:
CARL E. VUONO
General, United States Army
Chief of Staff
Official:

MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

History. This UPDATE printing publishes a revision that is effective 7 October 1988. This publication has been reorganized to make it compatible with the Army electronic publishing database. No content has been changed.

Summary. This regulation implements the Department of Defense and Department of the Army Personnel Security Program and takes precedence over all other departmental issuances affecting these programs. It contains the policies and procedures for access to classified information and assignment in a sensitive position. It also prescribes the investigative scope and adjudicative standards and criteria that are necessary prerequisites for such access or employment. It includes due process procedures for appealing adverse administrative actions rendered in accordance with the provisions of this regulation. This regulation contains all of DOD 5200.2–R and includes all recommendations of the Commission to Review DOD Security Policies and Practices (Stilwell Commission) approved for implementation. Army implementing instructions in this regulation are set in boldface type.

Applicability. This regulation applies to all military members of the Active Army, Army National Guard (ARNG), and U.S. Army Reserve (USAR), and civilian employees of the Army. It applies only to Army contractor personnel who require access to sensitive compartmented information in the performance of their duties.

Proponent and exception authority. Not applicable

Army management control process. This regulation is not subject to the requirements of AR 11–2. It does not contain internal control provisions.

Supplementation. Supplementation of this regulation is prohibited unless prior approval is obtained from HQDA (DAMI–CIS), WASH DC 20310–1051.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the Deputy Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI–CIS), WASH DC 20310–1051.

Distribution. Distribution of this publication is made in accordance with DA Form 12–9A–R requirements for 380 series publications. The number of copies distributed to a given subscriber is the number of copies requested in blocks 326, 327, 328, 329, and 330 of the subscriber's DA Form 12–9A–R. AR 380–67 distribution is A, B, C, D, and E for the Active Army, the ARNG, and the USAR. Existing account quantities will be adjusted and new account quantities will be established upon receipt of a signed DA Form 12–9U–R (Subscription for Army UPDATE Publications Requirements) from the publications account holder.

Contents (Listed by paragraph and page number)

Chapter 1
General Provisions, *page 1*

Section I
References, page 1
References • 1–100, *page 1*
Referenced forms • 1–101, *page 2*

Section II
Purpose and Applicability, page 2
Purpose • 1–200, *page 2*
Applicability • 1–201, *page 2*

Section III
Definitions, page 2
Access • 1–300, *page 2*
Adverse action • 1–301, *page 2*
Applicant • 1–301.1, *page 2*
Backround Investigation (BI) • 1–302, *page 2*
Classified information • 1–303, *page 2*
Close and continuous relationship • 1–303.1, *page 2*
Close foreign ties • 1–303.2, *page 2*
Compelling need • 1–303.3, *page 2*
Competent medical authority • 1–303.4, *page 3*
Defense Central Index of Investigations (DCII) • 1–303.5, *page 3*
Defense Central Security Index (DCSI) • 1–304, *page 3*
Denial of security clearance • 1–304.1, *page 3*
Department–determined personnel security status (DDPSS) • 1–304.2, *page 3*
Derogatory information • 1–304.3, *page 3*
DOD Component • 1–305, *page 3*
Entrance National Agency Check (ENTNAC) • 1–306, *page 3*
Federal service • 1–306.1, *page 3*
Head of DOD Component • 1–307, *page 3*
Immediate family • 1–307.1, *page 3*
Immigrant alien • 1–308, *page 3*
Interim security clearance • 1–309, *page 3*
Limited access authorization • 1–310, *page 3*
Local records check (LRC) • 1–310.1, *page 3*

*This regulation supersedes AR 604–5, 1 February 1984, and AR 614–3, 13 May 1985.

UNCLASSIFIED

Major Army command (MACOM) • 1–310.2, *page 3*
Minor derogatory information • 1–311, *page 3*
National Agency Check (NAC) • 1–312, *page 3*
National Agency Check and written inquiries (NACI) • 1–313, *page 3*
DOD National Agency Check and written inquiries (DNACI) • 1–314, *page 3*
National of the United States • 1–314.1, *page 3*
National security • 1–315, *page 3*
Need to know • 1–316, *page 4*
Periodic reinvestigation (PR) • 1–317, *page 4*
Personnel security • 1–317.1, *page 4*
Personnel security investigation (PSI) • 1–318, *page 4*
Polygraph examination • 1–318.1, *page 4*
Revocation of security clearance • 1–318.2, *page 4*
Scope • 1–319, *page 4*
Security clearance • 1–320, *page 4*
Senior Officer of the Intelligence Community (SOIC) • 1–321, *page 4*
Sensitive compartmented information (SCI) • 1–321.1, *page 4*
Sensitive position • 1–322, *page 4*
Significant derogatory information • 1–323, *page 4*
Special access program • 1–324, *page 4*
Special background investigation (SBI) • 1–325, *page 4*
Special investigative inquiry (SII) • 1–326, *page 4*
Specific geographic area • 1–326.1, *page 4*
Service • 1–327, *page 4*
Suspension of access • 1–327.1, *page 4*
Unfavorable administrative action • 1–328, *page 5*
Unfavorable personnel security determination • 1–329, *page 5*
United States citizen • 1–330, *page 5*

Chapter 2
Policies, *page 5*

Section I
Standards for Access to Classified Information or Assignment to Sensitive Duties, page 5
General • 2–100, *page 5*
Clearance and sensitive position standard • 2–101, *page 5*
Military service standard • 2–102, *page 5*

Section II
Criteria for Application of Security Standards, page 5
Criteria for application of security standards • 2–200, *page 5*

Section III
General • 2–300, *page 6*
National Agency Check/Entrance National Agency Check • 2–301, *page 6*
National Agency Check and written inquiries • 2–302, *page 6*
DOD National Agency Check and written inquiries • 2–303, *page 6*
Background investigation • 2–304, *page 6*
Special background investigation • 2–305, *page 6*
Special investigative inquiry • 2–306, *page 6*
Periodic reinvestigation • 2–307, *page 6*
Personal interview • 2–308, *page 6*
Expanded investigation • 2–309, *page 7*

Section IV
Authorized Personnel Security Investigative Agencies, page 7
General • 2–400, *page 7*
Subversive affiliations • 2–401, *page 7*
Suitability information • 2–402, *page 7*
Hostage situations • 2–403, *page 8*
Overseas personnel security investigations • 2–404, *page 8*

Section V
Limitations and Restrictions, page 8
Authorized requesters and personnel security determination authorities • 2–500, *page 8*
Limit investigations and access • 2–501, *page 8*
Collection of investigative data • 2–502, *page 8*
Privacy Act notification • 2–503, *page 8*
Restrictions on investigators • 2–504, *page 8*
Polygraph restrictions • 2–505, *page 8*

Chapter 3
Personnel Security Investigative Requirements, *page 9*

Section I
Sensitive Positions, page 9
Designation of sensitive positions • 3–100, *page 9*
Criteria for security designation of positions • 3–101, *page 9*
Authority to designate sensitive positions • 3–102, *page 9*
Limitation of sensitive positions • 3–103, *page 9*
Billet control system for TOP SECRET • 3–104, *page 9*

Section II
Civilian Employment, page 9
General • 3–200, *page 9*
Nonsensitive positions • 3–201, *page 9*
Exceptions to investigative requirements • 3–201.1, *page 9*
Noncritical–sensitive positions • 3–202, *page 10*
Critical–sensitive positions • 3–203, *page 10*
Exceptions • 3–204, *page 10*
Mobilization of DOD civilian retirees • 3–205, *page 10*

Section III
Military Appointment, Enlistment, and Induction, page 10
General • 3–300, *page 10*
Entrance investigation • 3–301, *page 10*
Reserve Components and National Guard • 3–302, *page 10*
Exceptions for certain commissioned officers of Reserve Components • 3–303, *page 10*
Mobilization of military retirees • 3–304, *page 11*
Mobilization exercises • 3–305, *page 11*

Section IV
Security Clearance, page 11
General • 3–400, *page 11*
Investigative requirements for clearance • 3–401, *page 11*
Naturalized U.S. citizens • 3–402, *page 11*
Access to classified information by non–U.S. citizens • 3–403, *page 11*
Access by persons outside the executive branch • 3–404, *page 12*
Restrictions on issuance of personnel security clearances • 3–405, *page 13*
Administrative downgrading • 3–405.1, *page 13*
Dual citizenship • 3–406, *page 13*
One–time access • 3–407, *page 13*
Access by retired flag/general officers • 3–408, *page 13*

Section V
Special Access Programs, page 14
General • 3–500, *page 14*
Sensitive compartmented information (SCI) • 3–501, *page 14*
Retired general officer (GO) SCI access determinations • 3–501.1, *page 16*
Single Integrated Operation Plan–extremely sensitive information (SIOP–ESI) • 3–502, *page 16*
Presidential support activities • 3–503, *page 16*
Nuclear weapon personnel reliability program (PRP) • 3–504, *page 16*
Chemical Personnel Reliability Program • 3–504.1, *page 17*
Automation security • 3–504.2, *page 17*

Access to North Atlantic Treaty Organization (NATO) classified information • 3–505, *page 17*
Other Special Access programs • 3–506, *page 17*

Section VI
Certain Positions Not Necessarily Requiring Access to Classified Information., page 17
General • 3–600, *page 17*
Access to restricted areas, sensitive information, or equipment not involving access to classified information • 3–601, *page 18*
Nonappropriated Fund employees • 3–602, *page 18*
Customs inspectors • 3–603, *page 18*
Red Cross/United Service Organizations personnel • 3–604, *page 18*
Officials authorized to issue security clearances • 3–605, *page 18*
Officials authorized to grant access to SCI • 3–605.1, *page 18*
Personnel security clearance adjudication officials • 3–606, *page 18*
Persons requiring DOD building passes • 3–607, *page 18*
Foreign national employees overseas not requiring access to classified information • 3–608, *page 18*
Special agents and investigative support personnel • 3–609, *page 18*
Persons requiring access to chemical agents • 3–610, *page 18*
Education and orientation personnel • 3–611, *page 18*
Contract guards • 3–612, *page 19*
Transportation of arms, ammunition and explosives (AA&E) • 3–613, *page 19*
Personnel occupying information systems positions designated ADP–I, ADP–II, and ADP–III • 3–614, *page 19*

Section VII
Reinvestigation, page 19
General • 3–700, *page 19*
Allegations related to disqualification • 3–701, *page 19*
Access to sensitive compartmented information (SCI) • 3–702, *page 19*
Critical–sensitive positions • 3–703, *page 19*
Critical military duties • 3–703.1, *page 19*
Presidential support duties • 3–704, *page 19*
NATO staff • 3–705, *page 20*
Extraordinarily sensitive duties • 3–706, *page 20*
Foreign nationals employed by DOD organizations overseas • 3–707, *page 20*
Persons accessing very sensitive information classified SECRET • 3–708, *page 20*
Access to TOP SECRET information • 3–709, *page 20*
Personnel occupying computer positions designated ADP–I • 3–710, *page 20*
Critical nuclear duty positions • 3–711, *page 20*

Section VIII
Authority to Waive Investigative Requirements, page 20
Authorized officials • 3–800, *page 20*
Combat operations, DA–directed mobilization • 3–801, *page 20*

Chapter 4
Reciprocal Acceptance of Prior Investigations and Personnel Security Determinations, *page 20*
General • 4–100, *page 20*
Prior investigations conducted by DOD investigative organizations • 4–101, *page 20*
Prior personnel security determinations made by DOD authorities • 4–102, *page 20*
Investigations conducted and clearances granted by other agencies of the Federal Government • 4–103, *page 21*

Chapter 5
Requesting Personnel Security Investigations, *page 21*
General • 5–100, *page 21*
Authorized requesters • 5–101, *page 21*
Criteria for requesting investigations • 5–102, *page 21*
Request procedures • 5–103, *page 21*
Priority requests • 5–104, *page 22*
Personal data provided by the subject of the investigation • 5–105, *page 22*
Requests for additional information or clarification • 5–106, *page 22*
Grounds for denial • 5–107, *page 22*
Requesting NACIs from OPM • 5–108, *page 23*

Chapter 6
Adjudication, *page 23*
General • 6–100, *page 23*
Central adjudication • 6–101, *page 23*
Evaluation of personnel security information • 6–102, *page 23*
Adjudicative record • 6–103, *page 24*
Reporting results of security or suitability determinations for civilian employees • 6–104, *page 24*

Chapter 7
Issuing Clearance and Granting Access, *page 24*
General • 7–100, *page 24*
Issuing clearance • 7–101, *page 24*
Granting access • 7–102, *page 25*
Administrative withdrawal • 7–103, *page 25*

Chapter 8
Unfavorable Administrative Actions, *page 25*

Section I
Requirements, page 25
General • 8–100, *page 25*
Referral for action • 8–101, *page 25*
Suspension • 8–102, *page 26*
Final unfavorable administrative actions • 8–103, *page 26*

Section II
Procedures, page 26
General • 8–200, *page 26*
Unfavorable administrative action procedures • 8–201, *page 26*
Requests for reconsideration • 8–201.1, *page 28*
Involuntary separation of military members and DA civilian personnel • 8–201.2, *page 28*
Exceptions to policy • 8–202, *page 28*

Section III
Reinstatement of Civilian Employees, page 28
General • 8–300, *page 28*
Reinstatement benefits • 8–301, *page 28*

Chapter 9
Continuing Security Responsibilities, *page 28*

Section I
Evaluating Continued Security Eligibility, page 28
General • 9–100, *page 28*
Management responsibility • 9–101, *page 28*
Supervisory responsibility • 9–102, *page 28*
Individual responsibility • 9–103, *page 29*
Coworker responsibility • 9–104, *page 29*

Section II
Security Education, page 29
General • 9–200, *page 29*
Initial briefing • 9–201, *page 29*

Contents—Continued

Refresher briefing • 9–202, *page 30*
Foreign travel briefing • 9–203, *page 30*
Termination briefing • 9–204, *page 30*

Chapter 10
Safeguarding Personnel Security Investigative Records, *page 30*
General • 10–100, *page 30*
Responsibilities • 10–101, *page 30*
Access restrictions • 10–102, *page 30*
Safeguarding procedures • 10–103, *page 31*
Records disposition • 10–104, *page 31*
Foreign source information • 10–105, *page 31*

Chapter 11
Program Management, *page 31*
General • 11–100, *page 31*
Responsibilities • 11–101, *page 31*
Reporting requirements • 11–102, *page 32*
Inspections • 11–103, *page 32*

Appendixes

A. References, *page 33*

B. Investigative Scope, *page 33*

C. Request Procedures, *page 36*

D. Tables for Requesting Investigations, *page 39*

E. Reporting of Nonderogatory Cases, *page 42*

F. Personnel Security Determination Authorities, *page 42*

G. Guidelines for Conducting Prenomination Personal Interviews, *page 42*

H. List of Designated Countries, *page 45*

I. Adjudication Policy, *page 45*

J. Overseas Investigations, *page 52*

K. ADP Position Categories and Criteria for Designating Positions, *page 54*

L. Defense Security Briefing Provided U.S. Government Employees Traveling to Communist–Controlled Countries, *page 55*

Glossary

Index

Chapter 1
General Provisions

Section I
References

1–100. References

a. DOD 5200.2–R, "DOD Personnel Security Regulation," December 1979 (Superseded), authorized by DOD Directive 5200.2, December 20, 1979

b. DOD 5220.22–R, "Industrial Security Regulation," December 1985, authorized by DOD Directive 5220.22, December 8, 1980. **AR 380–49 (Industrial Security)**

c. DOD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," August 12, 1985. **AR 380–49 (Industrial Security)**

d. **AR 380–35 (Department of the Army Communications Intelligence Security Regulation)**

e. Public Law 88–290, "National Security Agency—Personnel Security Procedures"

f. Public Law 86–36, "National Security Agency—Officers and Employees"

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

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

i. DOD Directive 5210.45, "Personnel Security in the National Security Agency," May 9, 1964

j. Executive Order 12356, "National Security Information," April 2, 1982

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

l. Director of Central Intelligence Directive (DCID) No. 1/14, "Minimum Personnel Security Standards and Practices Governing Access to Sensitive Compartmented Information," April 14, 1986

m. Privacy Act of 1974, Section 552a, Title 5, United States Code.

n. DOD Directive 5100.23, "Administrative Arrangements for the National Security Agency," May 17, 1967

o. Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction With the Federal Bureau of Investigation, April 5, 1979

p. DOD Directive 5210.48, "DOD Polygraph Program," December 24, 1984. **AR 195–6 (Department of the Army Polygraph Activities)**

q. DOD 5200.1–R, "Information Security Program Regulation," June 1986 authorized by DOD Directive 5200.1, "DOD Information Security Program," June 7, 1982. **AR 380–5 (Department of the Army Information Security Program Regulation)**

r. DOD Directive 5210.55, "Selection of DOD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activites," July 6, 1977

s. DOD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program," December 6, 1985. **AR 50–5 (Nuclear and Chemical Weapons and Materiel—Nuclear Surety)**

t. DOD Directive 5200.8, "Security of Military Installations and Resources," July 29, 1980. **AR 190–16 (Physical Security)**

u. DOD 1401.1–M, "Personnel Policy Manual for Nonappropriated Fund Instrumentalities," January 1981, authorized by DOD Instruction 1401.1, July 24, 1978. **AR 215–5 (Nonappropriated Funds Accounting Policy and Reporting Procedures)**

v. DOD 5030.49–R, "Customs Inspection," May 1977, authorized by DOD Directive 5030.49, January 6, 1984. **AR 190–41 (Customs Law Enforcement)**

w. DOD Directive 5210.25, "Assignment of American National Red Cross and United Service Organizations Inc. Employees to Duty with the Military Services," May 12, 1983. **AR 380–49 (Industrial Security)**

x. DOD Directive 5210.46, "Department of Defense Building Security for the National Capital Region," January 28, 1982. **AR 380–4 (Department of the Army Physical Security Program in the National Capital Region)**

y. DOD Directive 5210.65, "Chemical Agent Security Program," September 8, 1982. **AR 50–6 (Nuclear and Chemical Weapons and Materiel—Chemical Surety)**

z. DOD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978. **AR 380–150 (Access to and Dissemination of Restricted Data)**

aa. DOD Directive 5400.7, "DOD Freedom of Information Act Program," March 24, 1980. **AR 340–17 (Release of Information and Records from Army Files)**

bb. DOD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982. **AR 340–21 (The Army Privacy Program)**

cc. Federal Personnel Manual, chapter 732, subchapter 1, paragraph 1–6b **and chapters 731 and 736**

dd. Section 3571, Title 5, United States Code

ee. Section 3, Public Law 89–380

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

gg. Atomic Energy Act of 1954, as amended

hh. DOD Directive 5105.42, "The Defense Investigative Service," June 14, 1985

ii. Defense Investigative Service 20–1–M, "Manual for Personnel Security Investigations," July 1985

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

kk. USSAN Instruction 1–69, April 21, 1982 (Enclosure 2 to DOD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs" April 21, 1982). **(C) AR 380–15 (Safeguarding Classified NATO Information (U))**

ll. DOD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984. **(C) AR 380–10 (Disclosure of Information and Visits and Accreditation of Foreign Nationals (U))**

mm. DOD Directive 5100.3, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands," March 17, 1980

nn. Public Law 96–456, 95 Stat. 2025, "Classified Information Procedures Act of 1980"

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

pp. Section 7532, Title 5, United States Code

qq. **AR 190–56 (The Army Civilian Police and Security Guard Program)**

rr. **AR 381–12 (Subversion and Espionage Directed Against the U.S. Army) (SAEDA)**

ss. **AR 381–20 (U.S.Army Counterintelligence Activities)**

tt. **AR 381–45 (Investigative Records Repository)**

uu. **AR 600–31 (Suspension of Favorable Personnel Actions for Military Personnel in National Security Cases and Other Investigations and Proceedings)**

vv. **AR 600–37 (Unfavorable Information)**

ww. **AR 600–240 (Marriage in Oversea Commands)**

xx. **AR 608–10 (Military Personnel Security Program)**

yy. **AR 608–61 (Application for Authorization to Marry Outside the United States)**

zz. **AR 611–101 (Commissioned Officer Classification System)**

aaa. **AR 611–112 (Manual of Warrant Officer Military Occupational Specialties)**

bbb. **AR 611–201 (Enlisted Career Management Fields and Military Occupational Specialties)**

ccc. **AR 614–200 (Selection of Enlisted Soldiers for Training and Assignment)**

ddd. **AR 640–10 (Individual Military Personnel Records)**

eee. **CFR 213**
fff. **CPR 296–31**
ggg. **FPM Letter 732, November 14, 1978**
hhh. **OMB Circular A–71, July 1978**
iii. **OMB Circular A–130, December 12, 1985**

1–101. Referenced forms

a. **DA Form 477 (Requisition for Enlisted Personnel)**
b. **DA Form 872 (Requisition of Individual Officer Personnel)**
c. **DA Form 873 (Certificate of Clearance and/or Security Determination)**
d. **DA Form 2962 (Security Termination Statement and Debriefing Certificate)**
e. **DA Form 5247–R (Request for Security Determination (LRA)**
f. **DA Form 5248–R (Report of Unfavorable Information for Security Determination)**
g. **DD Form 398 (Personnel Security Questionnaire)**
h. **DD Form 398–2 (Personnel Security Questionnaire (National Agency Check))**
i. **DD Form 1879 (Request for Personnel Security Investigation)**
j. **DD Form 2221 (Authority for Release of Information and Records)**
k. **DD Form 2280 (Armed Forces Fingerprint Card)**
l. **FD 258 (Applicant Fingerprint Card)**
m. **FS–240 (Report of Birth Abroad of a Citizen of the United States of America)**
n. **FS–545 (Certification of Birth)**
o. **SF 85 (Data for Nonsensitive or Noncritical-Sensitive Position)**
p. **SF 87 (U.S. Civil Service Commission Fingerprint Chart)**
q. **SF 171 (Personnel Qualifications Statement)**

Section II
Purpose and Applicability

1–200. Purpose

a. To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces **and United States Army,** acceptance and retention of civilian employees in the Department of Defense (DOD) **and Department of the Army,** and granting members of the Amed Forces, **Army, DA and** DOD civilian employees, **DA and** DOD contractors, and other affiliated persons access to classified information **and assignment to sensitive positions** are clearly consistent with the interests of national security.

b. This regulation:

(1) Establishes DOD **and DA** personnel security policies and procedures;

(2) Sets forth the standards, criteria and guidelines upon which personnel security determinations shall be based;

(3) Prescribes the kinds and scopes of personnel security investigations required;

(4) Details the evaluation and adverse action procedures by which personnel security determinations shall be made; and

(5) Assigns overall program management responsibilities.

1–201. Applicability

a. This regulation implements the Department of Defense **and Department of the Army** Personnel Security Program and takes precedence over all other departmental issuances affecting that program.

b. All provisions of this regulation apply to **DA and** DOD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, **U.S. Army, DA and** contractor personnel and other personnel who are affiliated with the Department of Defense **and the Army** except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DOD 5220.22–R **(AR 380–49)** (reference (b)) and in DOD Directive 5220.6 **(AR 380–49)** (reference (c)).

c. The policies and procedures which govern the National Security Agency are prescribed by Public Laws 88–290 and 86–36, Executive Orders 10450 and 12333, DOD Directive 5210.45, Director of Central Intellignece Directive (DCID) 1/14 (references (e), (f), (g), (h), (i), and (l), repectively), and regulations of the National Security Agency.

d. Under combat conditions or other military exigencies, an authority in paragraph 1, appendix F, may waive such provisions of this regulation as the circumstances warrant.

e. **This regulation also applies to —**

(1) **Persons employed, hired on an individual basis, or serving on an advisory or consultant basis (including co–op and summer hire students) for whom Army personnel security clearances are required, whether or not such persons are paid from appropriated or nonappropriated funds.**

(2) **Employees of the Army National Guard, Army–Air Force Exchange Service, American Red Cross, the United Service Organizations (USO), who are required to have Army personnel security clearances.**

Section III
Definitions

1–300. Access

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

1–301. Adverse action

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

1–301.1. Applicant

A person not currently employed by the DA or serving in the Armed Forces, or a person being considered for employment for a sensitive position.

1–302. Backround Investigation (BI)

A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph B–3, appendix B, this regulation, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

1–303. Classified information

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

1–303.1. Close and continuous relationship

Persons to whom subject is bound by affection or obligation. May include sharing living quarters with an individual even though no intimate relationship exists.

1–303.2. Close foreign ties

Recurring contact, either personal or by correspondence, with foreign nationals residing in a foreign country.

1–303.3. Compelling need

Access to Sensitive Compartmented information (SCI) is urgently required by an individual to prevent failure or serious

impairment of missions or operations that are in the best interest of national security.

1–303.4. Competent medical authority
A board–eligible or board–certified psychiatrist or clinical psychologist employed by or under contract to the U.S. military or U.S. Government.

1–303.5. Defense Central Index of Investigations (DCII)
An alphabetical index of personal names and impersonal titles that appear as subjects of incidents in investigative documents held by the criminal, counterintelligence, fraud, and personnel security investigative activities of the Defense Investigative Service (DIS), the Defense Criminal Investigative Service (DCIS), and the NSA. DCII records will be checked on all subjects of DOD investigations.

1–304. Defense Central Security Index (DCSI)
An automated subsystem of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all DOD Components for military, civilian, and contractor personnel. The DCSI will serve as the central DOD repository of security–related actions in order to assist DOD security officials in making sound clearance and access determinations. The DCSI shall also serve to provide accurate and reliable statistical data for senior DOD officials, Congressional committees, the General Accounting Office and other authorized Federal requesters.

1–304.1. Denial of security clearance
The refusal to grant a security clearance or to grant a higher level of clearance to a person who possesses a clearance of a lower degree.

1–304.2. Department–determined personnel security status (DDPSS)
The highest level of personnel security eligibility to classified defense information granted by the Commander, U.S. Army Central Clearance Facility (CCF), based on the scope of a valid personnel security investigation on record. These data are determined in automated personnel data bases by the Commander, CCF.

1–304.3. Derogatory information
Information that constitutes a possible basis for taking an adverse or unfavorable personnel security action.

a. **Adverse loyalty information (see paras 2–200 *a–f*, 2–200 *k* , and app E, para 3).**

b. **Adverse suitability information (see paras 2–200 *g* through *j* and 2–200 *1* through *q* and app E, paras 1, 2, 4, 5, and 6).**

1–305. DOD Component
Includes the Office of the Secretary of Defense; The Military Departments; Organization of the Joint Chiefs of Staff; Directors of Defense Agencies and the United and Specified Commands.

1–306. Entrance National Agency Check (ENTNAC)
A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

1–306.1. Federal service
Federal service consists of active duty in the military services, Federal civilian employment, membership in the Army National Guard (ARNG) or U.S. Army Reserve (includes Troop Program Units, Individual Mobilization Augmentee (IMA), and Individual Ready Reserve), membership in the ROTC Scholarship Program, Federal contractor employment with access to classified information under the Industrial Security Program, or a combination thereof, without a break exceeding 12 months.

1–307. Head of DOD Component
The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands; and the Directors of Defense Agencies.

1–307.1. Immediate family
Includes subject's spouse, parents, brothers, sisters, and children.

1–308. Immigrant alien
Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

1–309. 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.

1–310. Limited access authorization
Authorization for access to CONFIDENTIAL or SECRET information granted to non–U.S. citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (app **J**).

1–310.1. Local records check (LRC)
A review of local personnel, post military police, medical records, and other security records as appropriate.

1–310.2. Major Army command (MACOM)
A command directly subordinate to, established by authority of, and specifically designated by HQDA. Army component of Unified and Specified Commands are MACOMs.

1–311. 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.

1–312. National Agency Check (NAC)
A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph 1, appendix B, this regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

1–313. National Agency Check and written inquiries (NACI)
A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

1–314. DOD National Agency Check and written inquiries (DNACI)
A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a NAC, a credit bureau check, and written inquiries to current and former employers (see para **B–**2, app B), covering a 5–year scope.

1–314.1. National of the United States
A citizen of the United States or a person who, though not a citizen, owes permanent allegiance to the United States. The provisions of this regulation are equally applicable to U.S. citizens and U.S. nationals.

1–315. National security
National security means the national defense and foreign relations of the United States.

1–316. Need to know
A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official U.S. Government program. Knowledge of, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

1–317. Periodic reinvestigation (PR)
An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs 3–700 through 3–711. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent 5–year period.

1–317.1. Personnel security
The application of standards and criteria to determine whether or not an individual is eligible for access to classified information, qualified for assignment to or retention in sensitive duties, and suitable for acceptance and retention in the total Army consistent with national security interests.

1–318. Personnel security investigation (PSI)
Any investigation required for the purpose of determining the eligibility of DOD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see para 2–403) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

1–318.1. Polygraph examination
A voluntary examination by qualified examiners using polygraph equipment approved by the DA. AR 195–6 (ref (p)) applies.

1–318.2. Revocation of security clearance
The cancellation of a person's eligibility for access to classified information.

1–319. Scope
The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

1–320. Security clearance
A determination that a person is eligible under the standards of this regulation for access to classified information.

1–321. Senior Officer of the Intelligence Community (SOIC)
The DOD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; Deputy Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

1–321.1. Sensitive compartmented information (SCI)
Classified information concerning or derived from intelligence sources, methods, or analytical processes that must be handled exclusively within formal access control systems established by the Director of Central Intelligence (DCI). DCI Directive (DCID) 1/14 (reference (1)) contains the minimum personnel security standards and procedures governing eligibility for access to SCI.

1–322. Sensitive position
Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical–sensitive, noncritical–sensitive, or nonsensitive as described in paragraph 3.

1–323. Significant derogatory information
Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

1–324. Special access program
Any program inposing "need–to–know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, OR TOP SECRET information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need to know.

1–325. Special background investigation (SBI)
A personnel security investigation consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph **B**–4, appendix B, this regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

1–326. Special investigative inquiry (SII)
A supplemental personnel security investigation of limited scope conducted to prove or disprove revelant 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.

1–326.1. Specific geographic area
The assignment location of a person. It is determined by the Commanding General, Total Army Personnel Agency (TAPA) with the Deputy Chief of Staff for Intelligence (DCSINT).

1–327. Service
Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DOD contractor or as a consultant involving access under the DOD Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months. **Service for nuclear and chemical surety positions is defined in AR 50–5 (reference (s)) and AR 50–6 (reference (y)) and in paragraph 3–504*a*(3)(g) of this regulation.**

1–327.1. Suspension of access
The temporary withdrawal of a person's eligibility for access to classified information. Access is suspended when information becomes known that casts doubt on whether continued access is consistent with national security interests.

1–328. Unfavorable administrative action

Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this regulation.

1–329. Unfavorable personnel security determination

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

1–330. United States citizen

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

b. ***Naturalized.*** **A person born outside of the United States who has completed naturalization procedures and has been given U.S. citizenship by duly constituted authority.**

c. ***Derivative birth.*** **A person born outside the United States who acquires U.S. citizenship at birth because one or both of his or her parents are U.S. citizens at the time of the person's birth.**

d. ***Derivative naturalization.*** **A person who acquires U.S. citizenship after birth through naturalization of one or both parents.**

Chapter 2
Policies

Section I
Standards for Access to Classified Information or Assignment to Sensitive Duties

2–100. General

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

b. **No person is entitled to knowledge of, possession of, or access to classified defense information solely by virtue of office, position, grade, rank, or security clearance. Such information will be entrusted only to persons whose official military or other governmental duties require it and who have been investigated and cleared for access under the standards prescribed by this regulation. Security clearances indicate that the persons concerned are eligible for access to classified information should their official duties require it.**

2–101. Clearance and sensitive position standard

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

2–102. Military service standard

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

Section II
Criteria for Application of Security Standards

2–200. Criteria for application of security standards

The ultimate decision in applying either of the security standards set forth in paragraphs 2–101 and 2–102, above, must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance **or assignment to a sensitive position** under the security standard shall include, but not be limited to the following:

a. Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

b. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

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

d. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or which seeks to overthrow the Government of the United States, or any State or subdivision thereof by unlawful means.

e. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by statute, Executive order, or regulation.

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

g. Disregard of public law, statutes, Executive orders, or regulations, including violation of security regulations or practices.

h. Criminal or dishonest conduct.

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

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

k. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be (1) the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States, or (2) any other circumstances that could cause the applicant to be vulnerable.

l. Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

m. Habitual or episodic use of intoxicants to excess.

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

o. Any knowing and willful falsification, coverup, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal agency.

p. Failing or refusing to answer or to authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment. **Refusing or intentionally failing to provide a current personal security questionnaire (PSQ) or omitting material facts in a PSQ or other security form. Refusing to submit to a medical or psychological evaluation when information indicates the individual may have a mental or nervous disorder or be addicted to alcohol or any controlled substance.**

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

Section III
Types and Scope of Personnel Security Investigations

2–300. General

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

2–301. National Agency Check/Entrance National Agency Check

Essentially, a NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making a personnel security determination. An ENTNAC is a NAC (scope as outlined in para **B**–1, app B) conducted on inductees and first–term enlistees, but lacking a technical fingerprint search. A NAC is also an integral part of each BI, SBI, and periodic reinvestigation (PR). Chapter 3 prescribes when a NAC is required.

2–302. National Agency Check and written inquiries

The Office of Personnel Management (OPM) conducts a NAC and written inquiries (NACI) on civilian employees for all departments and agencies of the Federal Government, pursuant to Executive Order 10450 (reference (g)). NACIs are considered to meet the investigative requirements of this regulation for a nonsensitive or noncritical–sensitive position and/or up to a SECRET clearance and, in addition to the NAC, include coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last 5 years.

2–303. DOD National Agency Check and written inquiries

DIS will conduct a DNACI, consisting of the scope contained in paragraph **B**–2, appendix B, for DOD military and contractor personnel for access to SECRET information. Chapter 3 prescribes when a DNACI is required.

2–304. Background investigation

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

2–305. Special background investigation

a. An SBI is essentially a BI providing additional coverage both in period of time as well as sources of information, scoped in accordance with the provisions of DCID ¼ (reference (l)) but without the personal interview. While the kind of coverage provided for by the SBI determines eligibility for access to SCI, DD has adopted this coverage for certain other Special Access programs. Chapter 3 prescribes when an SBI is required.

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

c. The detailed scope of an SBI is set forth in paragraph **B**–4, appendix B.

2–306. Special investigative inquiry

a. A Special investigative inquiry is a personnel security investigation conducted to prove or disprove allegations relating to the criteria outlined in paragraph 2–200 of this regulation, except current criminal activities (see para 2–402*d*), that have arisen concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a trustworthiness determination.

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

c. In those cases when there is a disagreement between Defense Investigative Service (DIS) and the requester as to the appropriate scope of the investigation, the matter may be referred to the Deputy Under Secretary of Defense for Policy for resolution. **Requests for resolution will be forwarded through command channels to HQDA (DAMI–CIS), Washington, DC 20310–1051.**

2–307. Periodic reinvestigation

As referred to in paragraph 3–700 and other national directives, certain categories of duties, clearance, and access require the conduct of a PR every 5 years according to the scope outlined in paragraph **B**–5, appendix B. The PR scope applies to military, civilian, contractor, and foreign national personnel.

2–308. Personal interview

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

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

b. Resolving adverse information. A personal interview of the subject shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DOD investigative organizations designated in this Regulation to conduct personnel security investigations), when necessary, as part of each special investigative inquiry, as well as during the course of initial or expanded

investigations, to resolve or clarify any information which may impugn the subject's moral character, threaten the subject's future Federal employment, raise the question of subject's security clearability, or be otherwise stigmatizing.

c. Hostage situation. A personal interview shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DOD investigative organizations designated in this regulation to conduct personnel security investigations) in those instances in which an individual has immediate family members or other persons bound by ties of affection or obligation who reside in a nation whose interests are inimical to the interests of the United States. (See para 2–403.)

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

(1) Existing personnel security screening systems (e.g., Air Force Assessment Screening Program, Naval Security Group Personnel Security Interview Program, U.S. Army Personnel Security Screening Program); or

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

(3) Agents of investigative agencies in direct support of the Component concerned.

e. Administrative procedures.

(1) The personal interview required by paragraph *d*, above, shall be conducted in accordance with appendix G.

(2) For those investigations requested subsequent to the personal interview requirements of paragraph *d*, above, the following procedures apply:

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

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

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

2–309. Expanded investigation

If adverse or questionable information relevant to a security determination is developed during the conduct of a personnel security investigation, regardless of type, the investigation shall be expanded, consistent with the restrictions in paragraph 2–504, to the extent necessary to substantiate or disprove the adverse or questionable information.

Section IV
Authorized Personnel Security Investigative Agencies

2–400. General

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

2–401. Subversive affiliations

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

(1) Overthrowing the Government of the United States or the government of a State;

(2) Substantially impairing for the purpose of influencing U.S. Government policies or decisions:

(a) The functions of the Government of the United States, or

(b) The functions of the government of a State;

(3) Depriving persons of their civil rights under the Constitution or laws of the United States.

b. Military Department/FBI jurisdiction. Allegations of activities covered by criteria *a* through *f* of paragraph 2–200 of this regulation are in the exclusive investigative domain of either the counterintelligence agencies of the Military Departments or the FBI, depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI (reference (o)). Whenever allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a personnel security investigation conducted by DIS, they shall be referred immediately to either the FBI or to a Military Department counterintelligence agency, as appropriate.

c. DIS jurisdiction. Allegations of activities limited to those set forth in criterion *g* through *q* of paragraph 2–200 of this regulation shall be investigated by DIS.

2–402. Suitability information

a. General. Most derogatory information developed through personnel security investigations of DOD military or civilian personnel is so–called suitability information, that is, information pertaining to activities or situations covered by criteria *g* through *q*of paragraph 2–200 of this regulation. Almost all unfavorable personnel security determinations made by DOD authorities are based on derogatory suitability information, although such information is often used as a basis for unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice or removal from Federal employment under OPM regulations.

b. Preclearance investigation. Derogatory suitability information, except that covered in *d*, below, developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel security clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to criteria *g* through *q* of paragraph 2–200.

c. Postadjudication investigation. Derogatory suitability allegations, except those covered by *d*, below, arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified information, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a special investigative inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior shall also be referred to DIS for investigation. In such cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when paragraph 3–701 applies. Postadjudication investigation of allegations of a suitability nature required to support other types of unfavorable

personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable Component administrative regulations. These latter categories of allegations lie outside the DOD personnel security program and are not a proper investigative function for departmental counterintelligence organizations, Component personnel security authorities, or DIS.

d. Allegations of criminal activity. Any allegations of conduct of a nature indicating possible criminal conduct, including any arising during the course of a personnel security investigation, shall be referred to the appropriate DOD, Military Department, or civilian criminal investigative agency. Military Department investigative agencies have primary investigative jurisdiction in cases where there is probable cause to believe that the alleged conduct will be the basis for prosecution under the Uniform Code of Military Justice. **Such information will be referred to the installation or unit provost marshal and/or security manager or the U.S. Army Criminal Investigation Command for action.**

2–403. Hostage situations

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

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

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

2–404. Overseas personnel security investigations

Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate Military Department investigative organization **(AR 381–20 (reference (ss)) applies).** Only postadjudication investigations involving an overseas subject may be referred by the requester directly to the Military Department investigative organization having investigative responsibility in the overseas area concerned (see app J) with a copy of the investigative request sent to DIS. In such cases, the Military Department investigative agency will complete the investigation and forward the completed report of investigation directly to DIS, with a copy to the requester.

Section V
Limitations and Restrictions

2–500. Authorized requesters and personnel security determination authorities

Personnel security investigations may be requested and personnel security clearances (including Special Access authorizations as indicated) granted only by those authorities designated in paragraph 5–101 and appendix F.

2–501. Limit investigations and access

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

2–502. Collection of investigative data

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

2–503. Privacy Act notification

Whenever personal information is solicited from an individual preparatory to the initiation of a personnel security investigation, the individual must be informed of (1) the authority (statute or Executive order that authorized solicitation); (2) the principal purpose or purposes for which the information is to be used; (3) the routine uses to be made of the information; (4) whether furnishing such information is mandatory or voluntary; (5) the effect on the individual, if any, of not providing the information; and (6) 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.

2–504. Restrictions on investigators

Investigation shall be carried out insofar as possible to collect only as much information as is relevant and necessary for a proper personnel security determination. Questions concerning personal and domestic affairs, national origin, financial matters, and the status of physical health thus should be avoided unless the question is relevant to the criteria of paragraph 2–200 of this regulation. Similarly, the probing of a person's thoughts or beliefs and questions about conduct that have no personnel security implications are unwarranted. When conducting investigations under the provisions of this regulation, investigators shall:

a. Investigate only cases or persons assigned within their official duties.

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

c. Always present credentials and inform sources of the reasons for the investigation. Inform sources of the subject's accessibility to the information to be provided and to the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisements to subjects of personnel security investigations are outlined in paragraph 2–503.

d. 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.

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

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

g. Refrain from conducting, under any circumstances, physical searches of the subject or his or her property.

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

2–505. 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, **(AR 195–6)** (reference (p)).

Chapter 3
Personnel Security Investigative Requirements

Section I
Sensitive Positions

3–100. Designation of sensitive positions

Certain civilian positions within the Department of Defense entail duties of such a sensitive nature, including access to classified information, that the misconduct, malfeasance, or nonfeasance of an incumbent in any such position could result in an unacceptably adverse impact upon the national security. These positions are referred to in this regulation as sensitive positions. It is vital to the national security that great care be exercised in the selection of individuals to fill such positions. Similarly, it is important that only positions which truly meet one or more of the criteria set forth in paragraph 3–101 be designated as sensitive. **A sensitive position will not be downgraded or reclassified as nonsensitive solely to aid in recruiting personnel.**

3–101. Criteria for security designation of positions

Each civilian position within the Department of Defense shall be categorized, with respect to security sensitivity, as either nonsensitive, noncritical–sensitive, or critical–sensitive.

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

(1) *Critical–sensitive.*

(a) Access to TOP SECRET information.

(b) Development or approval of plans, policies, or programs that affect the overall operations of the Department of Defense or of a DOD Component.

(c) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(d) Investigative and certain investigative support duties, the issuance **or adjudication** of personnel security clearances or access authorizations, or the making of personnel security determinations.

(e) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

(f) Duties falling under Special Access programs.

(g) Category I automated data processing (ADP) positions.

(h) Any other position so designated by the head of the Component or designee.

(2) *Noncritical–sensitive.*

(a) Access to SECRET or CONFIDENTIAL information.

(b) Security police/provost marshal–type duties involving the enforcement of law and security duties involving the protection and safeguarding of DOD personnel and property.

(c) Category II automated data processing positions.

(d) Duties involving education and orientation of DOD personnel.

(e) Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DOD personnel and property.

(f) Any other position so designated by the head of the Component or designee.

b. All other positions shall be designated as nonsensitive.

3–102. Authority to designate sensitive positions

The authority to designate sensitive positions is limited to those authorities designated in paragraph **F–7**, appendix F. These authorities shall designate each position within their jurisdiction as to its security sensitivity and maintain these designations current vis–a–vis the specific duties of each position.

3–103. Limitation of sensitive positions

It is the responsibility of those authorities authorized to designate sensitive positions to ensure that (1)only those positions that meet the criteria of paragraph 3–101,above,are designated as sensitive, and (2) the designation of sensitive positions is held to a minimum consistent with mission requirements. Designating authorities shall maintain an accounting of the number of sensitive positions by category, i.e., critical or noncritical–sensitive. Such information will be included in the annual report required in chapter 11.

3–104. Billet control system for TOP SECRET

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

b. Each request to DIS for a BI or SBI that involves access to TOP SECRET or SCI information will require inclusion of the appropriate billet reference, on the request for investigation.

Section II
Civilian Employment

3–200. General

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

3–201. Nonsensitive positions

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

3–201.1. Exceptions to investigative requirements

The following exceptions have been granted DA by the OPM:

a. **When a U.S. citizen or an alien scheduled to work in the United States and its territories or possessions is to be assigned to a nonsensitive position on a temporary basis not to exceed 6 months, a NACI is not automatically required. The commander or head of the activity will decide whether or not it is needed. In no case will this investigation be less than the preemployment inquiries prescribed by CPR 296–31, appendix B, S731–3 (reference (fff)). Commanders will ensure maximum and proper use of this exception.**

b. **A non–U.S. citizen to be assigned to a nonsensitive position outside the United States and its territories and possessions will be subject to as much of the investigation outlined below as it is feasible toconduct:**

(1) **A check of the national investigative agencies of the foreign government.**

(2) **A check of the appropriate local law enforcement agencies where the person has resided for the past 5 years.**

(3) **A check of the appropriate U.S. military intelligence files.**

c. **The requirement for the "written inquiries" portion of the NACI in connection with summer hire personnel has been**

waived. A NACI will be required if a summer hire employee is subsequently hired as a permanent employee.

d. **A NACI will not be requested for a military or civilian family member hired under 5 CFR 213.3106(b)(6) (reference (eee)). Commanders will ensure that this employment will not be adverse to U.S. interests.**

3–202. Noncritical–sensitive positions

a. An NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical–sensitive position (for exceptions see para 3–204). An ENTNAC, NAC or DNACI conducted during military or contractor employment may also be used for appointment provided a NACI has been requested from OPM and there is no more than 12 months break in service since completion of the investigation.

b. Seasonal employees (including summer hires) normally do not require access to classified information. For those requiring access to classified information, the appropriate investigation is required. The request for the NAC should be submitted to DIS by entering "SH" (summer hire) in red letters approximately 1 inch high on the DD Form 398–2, Personnel Security Questionnaire (National Agency Check). Additionally, to ensure expedited processing by DIS, summer hire requests should be assembled and forwarded to DIS in bundles, when appropriate.

3–203. Critical–sensitive positions

A BI shall be favorably completed prior to appointment to critical–sensitive positions (for exceptions see para 3–204). Certain critical–sensitive positions require a preappointment SBI in accordance with section V of this chapter. Preappointment BIs and SBIs will be conducted by DIS. **Inasmuch as a BI or SBI is of greater scope, a NACI will not be requested from OPM if a BI or SBI for employment in a critical–sensitive position is requested from DIS or a valid BI or SBI exists.**

3–204. Exceptions

a. Noncritical–sensitive. In an emergency, a noncritical–sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record **in the official personnel folder (OPF). The emergency finding will include a statement of why a delay pending completion of the required investigation will be harmful to the national interest.** In such instances, the position may be filled only after the NACI has been requested.

b. Critical–sensitive. In an emergency, a critical–sensitive position may be occupied pending completion of the BI (or SBI, as appropriate) if the head of the requesting organization **or an authority listed in paragraph F–7 *a*, appendix F** 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 the OPF. The emergency finding will include a statement of why a delay pending completion of the required investigation will be harmful to the national interest.** In such instances, the position may be filled only when the NAC portion of the BI (or SBI) or a previous valid NACI, NAC, or ENTNAC has been completed and favorably adjudicated, **and there has been no break in service in excess of 12 months.**

c. ***Harmful delays.*** **In exceptions *a* and *b* above, a delay in appointment may be considered harmful to national interests if the following apply:**

(1) **Regulatory requirements, mission–essential functions, or responsibilities cannot be met. A detailed explanation will be provided.**

(2) **No other personnel are available on a temporary basis to complete these requirements.**

d. ***Applicability.*** **This policy applies to new appointments and to current incumbents of positions when the sensitivity designation is changed.**

3–205. Mobilization of DOD civilian retirees

The requirements contained in paragraph 3–200 of this section, regarding the type of investigation required by position sensitivity for a DOD civilian retiree's temporary appointment when the break in employment is greater than 12 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of Title 5, United States Code, depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to newly assigned personnel assigned to the defense intelligence and security agencies with respect to granting security clearances in an expeditious manner under paragraph 3–200 of this section.

Section III
Military Appointment, Enlistment, and Induction

3–300. General

The appointment, enlistment, and induction of each member of the Armed Forces or their Reserve Components **into any of the components of the U.S. Army** shall be subject to the favorable completion of a personnel security investigation. The types of investigation required are set forth in this section.

3–301. Entrance investigation

a. An ENTNAC shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. A DNACI shall be conducted on each commissioned officer, warrant officer, cadet, midshipman, and Reserve Officers Training Candidate, at the time of **or before** appointment. **A SECRET clearance is a condition of appointment. Paragraph 3–303 outlines exceptions.** A full NAC shall be conducted upon reentry of any of the above when there has been a break in service greater than 12 months.

b. If an officer or warrant officer candidate has been the subject of a favorable NAC or ENTNAC and there has not been a break in service of more than 12 months, a new NAC is not authorized **and the NAC or ENTNAC may be used as the authority for commissioning, subject to favorable completion of a DNACI.** This includes ROTC graduates who delay entry onto active duty pending completion of their studies.

c. All derogatory information revealed during the enlistment or appointment process **(including Personnel Security Screening Program processing)** that results in a moral waiver will be fully explained on a written summary attached to the DD Form 398–2 **or DD Form 398.**

3–302. Reserve Components and National Guard

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

3–303. 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 DNACI provided that:

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

b. The applying health professional, chaplain, or attorney agrees in writing that, if the results of the investigation are unfavorable, he or she will be subject to discharge if found to be ineligible to hold a commission. Under this exception, commissions in Reserve Components other than the National Guard may be tendered to immigrant alien health professionals, chaplains, and attorneys; **however, provisions of paragraph 3–403 apply regarding eligibility for access to classified information.**

3–304. Mobilization of military retirees

The requirements contained in paragraph 3–301 of this section, regarding a full NAC upon reentry to active duty of any officer or enlisted regular/reserve military retiree or Individual Ready Reserve **(IRR)** who has been separated from service for a period of greater than 12 months **are** waived for the purposes of partial or full mobilization under provisions of Title 10, United States Code, to include the period of prescribed service refresher training. Particular priority should be afforded to military retirees mobilized and assigned to the defense intelligence and security agencies communities. **(See para 7–101 for issuance of interim clearances.)**

3–305. Mobilization exercises

MACOMs may waive the investigative requirements in paragraph 3–401 for any personnel under combat conditions or participating in HQDA–directed mobilization exercises. (See para 7–101 *e* for issuance of interim clearances.)

Section IV
Security Clearance

3–400. General

a. The authorities designated in paragraph **F–1,** appendix F, are the only authorities authorized to grant, deny or revoke DOD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.

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

c. **Before issuing any security clearance, final or interim, the commander must verify the following:**

(1) **That the person has had no break in Federal service exceeding 12 months since the completion of the investigation.**

(2) **That the person can prove U.S. citizenship by presenting one of the documents listed in paragraph B–4 *d* , appendix B (see para 3–402).**

3–401. Investigative requirements for clearance

a. TOP SECRET.

(1) Final clearance:

(a) BI **/SBI.**

(b) Established billet per paragraph 3–104 (except contractors).

(c) **Favorable review of local personnel, post military police, medical records, and other security records as appropriate.**

(2) Interim clearance:

(a) Favorable NAC, ENTNAC, DNACI, or NACI completed **within past 5 years.**

(b) Favorable review of DD Form 398/SF–86/SF–171/DD Form 49.

(c) BI or SBI has been initiated.

(d) Favorable review of local personnel, **post or** base military police, medical, and other security records as appropriate.

(e) Established billet per paragraph 3–104 (except contractors).

(f) Provisions of paragraph 3–204 have been met regarding civilian personnel.

(g) **If evidence exists of a BI, SBI, full field investigation, CID character investigation, or comparable investigation not over 4½ years old, provisions of subparagraphs (b) and (c) above are waived and a DA Form 5247–R (Request for Security Determination) requesting a final TOP SECRET clearance will be submitted to CCF noting that an interim clearance was granted. Such evidence will be attached to the DA Form 5247–R. CCF will check the DCII to find whether or not a later investigation exists that would require withdrawal of a security clearance.**

(h) **Commanders may grant an interim TOP SECRET clearance for 180 days in the name of the Commander, CCF.**

b. SECRET.

(1) Final clearance:

(a) DNACI: Military (except first–term enlistees) and contractor employees.

(b) NACI: Civilian employees.

1. **NACI is required even though the individual held a valid security clearance based on a NAC, ENTNAC, or DNACI while a member of the Armed Forces.**

2. **Exception: Summer hires, members of cooperative education programs, employees of nonappropriated fund instrumentalities, Army and Air Force Exchange Service employees, Red Cross members, USO employees, and non–Federal employees of the Army National Guard may be granted a final clearance on the basis of a favorable completed NAC/ENTNAC conducted by the DIS. No interim clearance is authorized for these employees.**

(c) Entrance: First–term enlistees.

(d) **Favorable review of local personnel, post military police, medical, and other security records as appropriate.**

(2) Interim clearance:

(a) When a valid need to access SECRET information is established, an interim SECRET clearance may be issued **for 180 days in the name of the Commander, CCF,** in every case, provided that a DA Form 5247–R has been submitted to CCF, and the steps outlined in subparagraphs (b) through (e) below, have been complied with.

(b) Favorable review of DD Form 398–2/SF 85/SF 171/DD Form 48.

(c) NACI, DNACI, or ENTNAC initiated.

(d) Favorable review of local personnel, **post or** base military police, medical, and **other** security records as appropriate.

(e) **NAC or ENTNAC completed or, in an emergency,** provisions of paragraph 3–204 have been complied with regarding civilian personnel.

c. CONFIDENTIAL.

(1) Final clearance:

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

(b) NACI; Civilian employees (except for summer hires **and others listed in para 3–401 *b* (l)(b)(l) *2* who may be granted a final clearance on the basis of a NAC).**

(c) **Favorable review of local personnel, post military police, medical, and other security records as appropriate.**

(2) Interim clearance:

(a) Favorable review of DD Form 398–2/SF 86/S171/DD Form 48.

(b) NAC, ENTNAC, or NACI initiated.

(c) Favorable review of local personnel, **post or** base military police, medical, and **other** security records as appropriate.

(d) Provisions of paragraph 3–204 have been complied with regarding civilian personnel.

d. Validity of, previously granted clearances. Clearances granted under less stringent investigative requirements retain their validity; however, if a higher degree of clearance is required, investigative requirements of this regulation will be followed.

3–402. Naturalized U.S. citizens

This paragraph rescinded per DUSD(P) memorandum dated 12 February 1988, subject: Revocation of the Policy, in paragraph 3–402, DOD 5200.2–R.

3–403. Access to classified information by non–U.S. citizens

a. Only U.S. citizens are eligible for a security clearance. Therefore, every effort shall be made to ensure that non–U.S. citizens are

not employed in duties that may require access to classified information. However, when there are compelling reasons to grant access to classified information to an immigrant alien or a foreign national in furtherance of the mission of the Department of Defense, such individuals may be granted a "limited access authorization" (LAA) under the following conditions:

(1) LAAs will be limited to SECRET and CONFIDENTIAL level only; LAAs for TOP SECRET are prohibited.

(2) Access to classified information is not inconsistent with that determined releasable by designated disclosure authorities, in accordance with DOD Directive 5230.11 **(AR380–10)** (reference (ll)) to the country of which the individual is a citizen.

(3) Access to classified information must be limited to information relating to a specific program or project.

(4) Favorable completion of a BI (scoped for 10 years); where the full investigative coverage cannot be completed, a counterintelligence scope polygraph examination will be required in accordance with the provisions of DOD Directive 5210.48 **(AR195–6)** (reference (p)).

(5) Security clearances previously issued to immigrant aliens will be reissued as LAAs. **Immigrant aliens who are eligible for U.S. citizenship and have not tried to become naturalized within 12 months of eligibility will not be considered for an LAA. They will be reported to CCF for action under chapter 8, if appropriate.**

(6) The limited access authorization determination shall be made only by an authority designated in paragraph **F–2**, appendix F.

(7) LAAs issued by the Unified and Specified Commands shall be reported to the central adjudicative facility of the appropriate Military Department in accordance with the assigned responsibilities in DOD Directive 5100.3 (reference (mm)) for inclusion in the Defense Central Index of Investigation (DCII).

(8) **LAAs will be limited to persons who have a special skill or technical expertise essential to the national security that is not available from U.S. personnel. LAAs will not be granted to secretarial or clerical personnel or others who perform routine administrative duties.**

(9) **Commanders are reminded that an LAA is not a security clearance but an authorization for access to specific, U.S. classified information required in performance of job duties. Exposure to classified information outside the scope of an approved LAA is a compromise of such information and will be processed according to AR 380–5 (reference (q)).**

b. In each case of granting a limited access authorization, a record shall be maintained as to:

(1) The identity (including current citizenship) of the individual to whom the limited access authorization is granted, to include, name and date and place of birth;

(2) Date and type of most recent investigation to include the identity of the investigating agency;

(3) The nature of the specific program material(s) to which access is authorized (delineated as precisely as possible);

(4) The classification level to which access is authorized;

(5) The compelling reasons for granting access to the materials cited in (3) above and

(6) Status of the individual (i.e., immigrant alien or foreign national).

c. Individuals granted LAAs under the foregoing provisions shall be the subject of a 5–year periodic reinvestigation as set forth in paragraph B–5, appendix B.

d. Foreign nationals who are LAA candidates must agree to submit to a counterintelligence–scope polygraph examination prior to being granted access in accordance with DOD Directive 5210.48 **(AR 195–6)**(reference (p)).

e. If geographical and political situations prevent the full completion of the BI (and/or counterintelligence–scope polygraph), issuance of an LAA shall not be authorized; exceptions to the policy may only be authorized by the DUSD(P).

f. A report on all LAAs in effect, including the data required in paragraph *b*(l) through (6) above, shall be furnished to the Deputy Under Secretary of Defense for Policy, **DCSINT (DAMI–CIS),** within **30** days after the end of each fiscal year (See para 11–102.)

3–404. Access by persons outside the executive branch

a. Access to classified information by persons outside the executive branch shall be accomplished in accordance with chapter VII, DOD 5200.1–R **(AR380–5)** (reference (q)). The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

b. Members of the U.S. Senate and House of Representatives do not require personnel security clearances, They may be granted access to DOD classified information which relates to matters under the jurisdiction of the respective committees to which they are assigned and is needed to perform their duties in connection with such assignments.

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

d. State Governors do not require personnel security clearances. They may be granted access to specifically designated classified information, on a "need– to–know" basis, based upon affirmation by the Secretary of Defense, **the Secretary of the Army, or the DCSINT** that access, under the circumstances, serves the national interest. Staff personnel of a Governor's office requiring access into classified information shall be investigated and cleared in accordance with the prescribed procedures of this regulation when the head of a DOD Component or single designee, **the Secretary of the Army, or the DCSINT** affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a "need–to–know" basis. **Requests for access by State Governors and/or the staff of a Governor's office will be submitted to HQDA (DAMI–CIS.)**

e. Members of the U.S. Supreme Court, the Federal judiciary and the Supreme Courts of the individual States do not require personnel security clearances. They may be granted access to DOD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

f. Attorneys representing DOD military, civilian or contractor personnel, requiring access to DOD **or DA** classified information to properly represent their clients, shall normally be investigated by DIS and cleared in accordance with the prescribed procedures in paragraph 3–401. This shall be done upon certification of the General Counsel of the DOD Component involved in the litigation **or Office of The Judge Advocate General** that access to specified classified information, on the part of the attorney concerned, is necessary to adequately represent his or her client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of paragraph 3–401, access may be granted with the written approval of an authority designated in **paragraph F–1,** appendix F, provided that as a minimum: (a) a favorable name check of the FBI and the DCII has been completed, and (b) a DOD Non–Disclosure Agreement has been executed. **Requests for access for attorneys representing DA military, civilian, or contractor personnel will be submitted through the Office of The Judge Advocate General (DAJA–AL), Washington, DC 20310–2212 to the Office of The Deputy Chief of Staff for Intelligence (DAMI–CIS), Washington, DC 20310–1056.** In postindictment cases, after a judge has invoked the security procedures of **Public Law 96–456, Stat. 2025,** the Classified Information Procedures Act (CIPA) (reference (nn)), the Department of Justice may elect to conduct the necessary background investigation and issue the required security clearance, in coordination with the affected DOD Component **or the DA.**

3–405. Restrictions on issuance of personnel security clearances

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

Personnel security clearances shall *not* be issued:

a. To persons in nonsensitive positions.

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

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

d. 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.

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

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

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

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

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

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

k. To drivers, chauffeurs and food service personnel.

3–405.1. Administrative downgrading

Clearance certificates (DA Form 873) will not be administratively reduced or invalidated because a person has been assigned to duties that do not require access to the same or lower degree of classified information, the permanent duty station has been changed, or to avoid revocation in the face of credible derogatory information.

3–406. Dual citizenship

Persons claiming both U.S. and foreign citizenship shall be processed under paragraph 3–401, above, and adjudicated in accordance with the "Foreign Preference" standard in appendix I.

3–407. One–time access

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

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

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

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

d. 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.

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

f. Whenever possible, access shall be confined to a single instance or, at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of the granting authority is required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be canceled at or before 90 days from original date of access.

g. 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.

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

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

(1) The name and SSN of the employee afforded higher level access.

(2) The level of access authorized.

(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.

(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.

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

(6) The approving authority's signature certifying (1) through (5), above.

(7) Copies of any pertinent briefings/debriefings administered to the employee.

3–408. Access by retired flag/general officers

a. Upon determination by an active duty flag/general officer that there are compelling reasons, in furtherance of the Department of Defense **or DA** mission, to grant a retired general officer access to classified information in connection with a specific DOD **or DA** program or mission, for a period not greater than 90 days, the investigative requirements of this regulation may be waived. The access shall be limited to classified information at a level commensurate with the security clearance held at the time of retirement—not including access to SCI. **This level of access may be determined by contacting the Commander, CCF (PCCF–SC).**

b. The flag/general officer approving issuance of the clearance shall provide the **CCF** a written record to be incorporated into the DCII detailing:

(1) All data pertaining to the cleared subject;

(2) The classification of the information to which access was authorized.

c. Such access may be granted only after the compelling reason and the specific aspect of the DOD **or DA** mission which is served by granting such access has been detailed and under the condition that the classified materials involved are not removed from the

confines of a Government installation or other area approved for storage of DOD **or DA** classified information.

Section V
Special Access Programs

3–500. General

It is the policy of the Department of Defense to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding established requirements are authorized only when mandated by statute, national regulations, or international agreement. In this connection, there are certain Special Access programs originating at the national or international level that require personnel security investigations and procedures of a special nature. These programs and the special investigative requirements imposed by them are described in this section. A Special Access program is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to section 4–2 of Executive Order 12356 (reference (j)) and prior orders. DOD 5200.1–R **(AR380–5)**(reference (q)) governs the establishment of Departmental Special Access Programs.

3–501. Sensitive compartmented information (SCI)

a. ***Investigative requirement.***The investigative requirement for access to SCI is an SBI (see para **B**–4, app B) including a NAC on the individual's spouse or cohabitant. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudication agency that the personnel security standards of DCID 1/14 (reference (l)) are met.

(1) **The individual must not be under flagging action under AR 600–31 (reference (fff)).**

(2) **The individual must not be under psychiatric care or participating in any drug or alcohol rehabilitation treatment.**

(3) **The individual must have no pending action under chapter 8 of this regulation.**

(4) **The individual must not be the defendant in any pending civil litigation.**

(5) **The individual and spouse, parents,brother, sister, children, or other persons with whom the individual cohabits or is bound by affection or obligation must be U.S. citizens. Requests for waiver of this criterion must justify a compelling operational requirement and be forwarded to CCF for approval with the SBI packet attached.(See *d,* below, for specific guidelines concerning foreign national affiliations.)**

(6) **Unresolved or unsubstantiated derogatory allegations should not normally be used to disqualify an individual without a complete investigation. Information of this type will be adjudicated by CCF after completion of the investigation. If the commander decides that the derogatory information clearly warrants denial of SCI access, the nomination and the derogatory information will be forwarded to CCF with the SBI packet attached.**

b. ***Previous investigations.*** A previous investigation conducted within the past 5 years which substantially meets the investigative requirements prescribed by this section may serve as a basis for granting access approval provided that there has been no break in the individual's military service, DOD civilian employment, or access to classified information under the Industrial Security Program greater than 12 months. **If the last SBI is more than 3 years old,** the individual shall submit one copy of an updated PSQ covering the period since the completion of the last SBI **to the servicing SSO for review.**

c. ***Nomination procedures.*** **An individual requiring SCI access should be nominated to CCF as soon as he or she is identified to fill an approved billet. Nominations will be submitted in accordance with AR 380–35 (reference (d)). If appropriate, nomination will certify that a review of the PSQ revealed no unfavorable information, or forward a copy of DD Form 398.**

(1) ***"One–time" access.*** **Exceptions are nominations for "one–time" SCI access to attend a conference or briefing, or other situation in which temporary (no more than 90 days) SCI access appears warranted. Normal SCI investigative standards (SBI completed within the last 5 years) apply in cases involving one–time access.**

(2) ***Exceptional circumstances.*** **Interim SCI access may be granted by the Commander, CCF, before completion of the fully prescribed investigation when the need for access to SCI is so urgent that the benefits would far outweigh the security risk. Requests for interim access are based on compelling need (see *d* (l)(c) below). Requests for exceptions must clearly state the compelling need and describe how denial of access will affect the ability of the organization to accomplish its mission.**

d. ***DCID 1/14 requirements.*** **DCID 1/14, paragraph 5b,equires that both the subject and members of his or her immediate family or cohabitant be U.S. citizens. Immediate family members, cohabitant, and persons to whom the subject is bound by affection or obligation should neither be subject to physical, mental, or other forms of duress by a foreign power, or advocate the use of force or violence to overthrow the Government of the United States by unconstitutional means.**

e. ***Foreign affiliation.*** **Individuals who are not U.S. citizens or who claim both U.S. and foreign citizenship are not eligible for SCI access. In addition, established criteria normally will not be waived if—**

(1) **Subject is a U.S. citizen but has resided in a country listed in appendix H for a significant period and/or has close foreign ties with relatives or associates residing in such a country. Whether or not such association is extensive or a risk to security depends on the nature and degree of contact and the potential for adverse influence or duress.**

(2) **Although a naturalized U.S. citizen,subject was born in a country listed in appendix H and has had extensive travel that was not a result of directed Federal service or has lived in or near the native country after obtaining U.S. citizenship.**

f. ***Family members with foreign affiliation.*** **A nominee who has parents, brothers, sisters, or children who are not U.S. citizens is not eligible for SCI unless CCF grants a waiver. The DCID 1/14 criteria may be waived in the absence of a compelling need, provided there is no evidence of anti–American feeling, and the family members were—**

(1) **Born in a country not listed in appendix H and live in the United States or in a country not listed in appendix H.**

(2) **Born in a country listed in appendix H but have not lived under a Communist regime, have no close ties with anyone living in a country listed in appendix H, and live in the United States.**

g. ***Spouse with foreign affiliation.*** **A nominee who is currently married to a foreign national is normally not eligible for SCI access. The prenomination interview required by paragraph 2–308 should reveal the affiliation and will normally preclude further processing of the SBI paperwork to DIS. This is particularly true when the nominee is identified by the losing command as requiring SCI access for a projected assignment. The losing command cannot determine the existence of a compelling need at the gaining command. When this situation arises, the losing command will immediately notify TAPA and suspend SCI processing pending notification by TAPA.**

(1) **The DCID 1/14 criteria may be waived if the commander (05 or above) certifies a compelling need exists and the following factors apply:**

(a) **Spouse was born in a country other than those listed in appendix H.**

(b) **There is no evidence of anti–American feeling demonstrated by spouse.**

(c) **A statement is submitted to CCF indicating that spouse intends to become a U.S. citizen, when eligible.**

(2) **The DCID 1/14 criteria may be waived for a non–U.S.**

citizen spouse from a country listed in appendix H provided the spouse has not lived for any significant period under a terrorist or Communist regime, has no close ties in such countries, and the supported command shows a compelling need for the nominee to have SCI access (see *d* (l)(c) above). There must be no evidence that the spouse has anti–American feelings. A statement must have been submitted indicating intent to apply for U.S. citizenship as soon as eligible.

(3) **Established criteria normally may not be waived if the following factors apply:**

(a) **Spouse was born in a country listed in appendix H and has resided under a terrorist or Communist regime with interests adverse to those of the United States for a significant period and/or maintains close ties with anyone in a country listed in appendix H. The fact that the spouse has obtained U.S. citizenship does not alter the circumstances.**

(b) **Spouse is eligible for U.S. citizenship, but has not tried to apply within 12 months of eligibility.**

(4) **The circumstances described above that apply to foreign–born spouses apply equally to subjects who share living quarters or cohabitate with foreign nationals.**

(5) **Nominees for whom a foreign national spouse waiver is granted under subparagraph 3–501 *g* may not be transferred in status, recertified to a gaining command, or extended in their present assignment without prior authorization from CCF.**

h. ***Waiver of foreign connections.*** **Requests for waiver of foreign connections for personnel in career management field (CMF) 33 or 98 need not be accompanied by a compelling need statement. Possession of CMF 33 or 98 is considered a compelling need because of the extreme shortage of personnel in these CMFs. However, all other requirements of *i* , below, apply. If CCF grants a waiver, these individuals may retain their SCI access eligibility upon transfer outside the foreign spouse's country of origin, may extend their foreign duty tour within the spouse's country of origin up to 4 years, and may be reassigned to spouse's country of origin provided spouse has applied for U.S. citizenship within 12 months of becoming eligible. Individuals in CMF 33 and 98 may be recertified to the gaining command for SCI access without prior authorization from CCF provided the spouse has applied for U.S. citizenship within 12 months of becoming eligible.**

i. ***Marriage to a foreign national.*** **The following measures apply to individuals indoctrinated for SCI access who plan to marry a non–U.S. citizen:**

(1) **An individual who declares an intent to marry a foreign national will immediately receive a command interview. Results of the interview stating whether or not a waiver will be requested will be forwarded to CCF and will cover the following information:**

(a) **Full name, date and place of birth, occupation, and citizenship of the prospective spouse and his or her family members.**

(b) **Whether or not the prospective spouse has had any connections with a hostile intelligence service or has any friends, relatives, or contacts residing in a country listed in appendix H.**

(c) **If the prospective spouse or a family member was born in what is now a country listed in appendix H, the dates, method, and circumstances of his or her departure from that country and the nature and extent of all ties remaining in that country will be fully determined.**

(d) **Whether or not the prospective spouse or any family member has expressed any unusual interest in the subject's assignments and/or duty position.**

(e) **Acknowledgment that the person understands the obligation to report any situation of potential Subversion and Espionage Directed Against U.S. Army and Deliberate Security Violations (SAEDA) interest under provisions of AR 381–12 (reference (rr)).**

(2) **If the command interview is favorable and the subject does not request a waiver or no compelling need for continuing access exists, the subject may remain indoctrinated until the marriage. At that time, the subject will be debriefed.**

(3) **If the subject wants to request a waiver and a compelling need exists, the request will be submitted through command channels to CCF. To permit continuous uninterrupted access, allow at least 6 months to process the waiver request and conduct the premarital investigation. The process involves the following actions:**

(a) **The command must certify that a compelling need exists and that a waiver is essential to the command's mission (or provide a statement that the person is in CMF 33 or 98) and furnish results of the command interview conducted under provisions of *i* (l) above.**

(b) **The person submitting the waiver request must furnish the following:**

1. **A statement that he or she understands that should the waiver be granted, he or she cannot be reassigned to the spouse's country of origin in a position requiring SCI access until the spouse has obtained U.S. citizenship, cannot be reassigned to a position requiring SCI access when a compelling need does not exist, and cannot request extension of a foreign service tour and retain SCI access unless exceptional circumstances involving operational deficiencies exist. (See *h* , above, for exception for CMF 33 and 98.)**

2. **A current DD Form 398–2, or its dual–language equivalent, completed by the prospective spouse.**

3. **A statement by the prospective spouse indicating an intention to become a U.S. citizen when eligible.**

4. **If the person is assigned to an overseas command, the command endorsement of the waiver request will include a copy of the investigation completed on the spouse in accordance with paragraph 6, AR 608–61 (reference (yy)), and paragraph 4, AR 600–240 (reference (ww)). These premarital investigations will essentially be at least equal to a foreign–country NAC, which includes investigative checks of national and local security and law enforcement agencies as well as other appropriate civil authorities in the place where the prospective spouse has resided since age 16 (CIA check will be requested by CCF, if required).**

5. **If the person is assigned to a continental United States (CONUS) command, CCF will use the DD Form 398–2 submitted with the waiver request to obtain appropriate CIA, Immigration and Naturalization Service (INS), and FBI checks on the prospective spouse. This will be the only investigation required unless adverse information is found during the processing and/or investigation.**

(c) **The person need not be debriefed from SCI access upon marriage to a foreign national if the requirements of this paragraph are met. If the command interview, review of the premarital investigation of the spouse, or review of DD Form 398–2 reveals information indicating a potential hostage situation, a SAEDA attempt, or possible connections with a hostile intelligence service, access will be suspended pending final determination by CCF and action under AR 381–12 (reference (rr)), if appropriate.**

(4) **If a person marries a foreign national without complying with the provisions outlined in *i* (3)(a) and (b), above, he or she is ineligible for continued SCI access and will be debriefed. The Special Security Officer (SSO) will tell CCF why the individual has been debriefed.**

(5) **When the spouse obtains U.S. citizenship, proof of citizenship must be presented to the supporting SSO. The SSO will immediately certify the following information to the CCF:**

(a) **Spouse's full identifying data.**

(b) **Date and place of entry of spouse into the United States.**

(c) **Naturalization certificate number.**

(d) **Date, court, and place of naturalization.**

(e) **Complete personal identifying data of the indoctrinated person.**

j. ***Close and continuous contact.*** **A person who establishes a close and continuous contact with a foreign national will have his or her SCI access suspended if there is reason to believe that**

the foreign national is involved with hostile intelligence, has connections in a country listed in appendix H, or is working for a foreign government in some capacity that may present a security threat. In the absence of those conditions, suspension may not be appropriate. The person should be counseled on his or her security responsibilities and given a SAEDA briefing. A report of the command's action will be sent to the CCF.

k. ***Other conditions.*** **CCF will be promptly notified if any of the following conditions become known or a matter of record:**

(1) **Adverse information reported or developed concerning the person or spouse.**

(2) **Spouse's refusal to apply, procrastination, or any other action that delays obtaining a U.S. citizenship.**

(3) **Spouse has or is suspected of having committed, on behalf of a foreign power, any act that is contrary to the best interest of the United States. The details of the situation will be immediately reported to the CCF and will include the person's degree of access to any compartment operation or project. No further action will be taken pending receipt of instructions from the CCF unless the security of SCI is endangered.**

l. ***Status of waiver.*** **CCF correspondence approving a waiver will advise whether or not the individual may be recertified to the gaining command for SCI access upon completion of current assignment without prior authorization from the CCF. The losing SSO's message to the gaining SSO will clearly state that the subject is married to a foreign national and whether or not CCF instructions allow a transfer in status.**

3–501.1. Retired general officer (GO) SCI access determinations

a. **A retired GO may participate in activities requiring one–time SCI access under the provisions of AR 380–35 (reference (d)) under the following conditions:**

(1) **The GO has a favorably completed SBI that meets the standards of DCID 1/14 at the time the investigation was completed.**

(2) **The GO is officially representing the U.S. Government at the request of an authorized U.S. Government agency. Such access is not authorized when the GO is representing a U.S. Government contractor, consulting firm, independent business, or the retired GO.**

(3) **No disqualifying information is available that would preclude granting SCI access.**

b. **An active duty GO whose SBI exceeds the 5–year–expiration period and who states an intention to retire within 6 months will not be required to have an SBI PR. However, such a GO will be encouraged to submit a request for an SBI PR because it would be advantageous to the Army and the GO to maintain current SCI eligibility.**

3–502. Single Integrated Operation Plan–extremely sensitive information (SIOP–ESI)

The investigative requirement for access to SIOP–ESI is an SBI, including a NAC on the spouse and the individual's immediate family who are 18 years of age or over and who are U.S. citizens other than by birth or who are resident aliens.

3–503. Presidential support activities

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

(1) *Category One*

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

1. Presidential aircrew and associated maintenance and security personnel.

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

3. White House transportation personnel.

4. Presidential mess attendants and medical personnel.

5. Other individuals filling administrative positions at the White House.

(b) Personnel assigned on a temporary or part–time basis to duties supporting the President:

1. Military social aides.

2. Selected security, transportation, flightline safety, and baggage personnel.

3. Others with similar duties.

(c) Personnel assigned to the Office of the Military Aide to the Vice President.

(2) *Category Two*

(a) Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential functions and facilities.

(b) Employees of contractors who provide services or contractors employees who require unescorted access to Presidential support areas, activities, or equipment, including maintenance of the Presidential retreat, communications, and aircraft.

(c) Individuals in designated units requiring a lesser degree of access to the President or Presidential support activities.

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

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

d. The U.S. citizenship of foreign–born immediate family members of all Presidential support nominees must be verified by investigation.

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

3–504. Nuclear weapon personnel reliability program (PRP)

a. DOD Directive 5210.42 **(AR 50–5)** (reference (s)) sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and nuclear components. The investigative requirement for personnel performing such duties is:

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

(a) The individual has had a favorable DNACI or NAC (or ENTNAC) within the past 5 years without a break in **active** service or employment in excess of 1 year.

(b) The BI has been requested.

(c) All other requirements of the PRP screening process have been fulfilled.

(d) The individual is identified to supervisory personnel as being certified on an interim basis.

(e) The individual is not used in a two–man team with another such individual.

(f) Justification of the need for interim certification is documented by the certifying official.

(g) Should the BI not be completed within 150 days from the date of the request, the certifying official shall query the Component clearance authority **(by forwarding DA Form 5247–R to the Commander, CCF (PCCF–M)),** who shall ascertain from DIS the status of the investigation. On the basis of such information, the certifying official shall determine whether to continue or to withdraw the interim certification.

(2) *Controlled position: DNACI/NACI* .

(a) An ENTNAC completed for the purpose of first–term enlistment or induction into the Armed Forces does not satisfy this requirement.

(b) Interim certification is authorized for an individual who has not had a DNACI/NACI completed within the past 5 years, subject to the following conditions:

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

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

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

4. Should the DNACI/NACI not be completed within 90 days from the date of the request, the procedures set forth in *a*(l)(g), above, for ascertaining the delay of the investigation in the case of a critical position shall apply.

(3) Additional requirements apply.

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

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

(c) **Periodic reinvestigation is required every 5 years for individuals assigned to critical nuclear weapon positions. PR is not required subsequent to initial assignment to PRP for controlled nuclear weapon positions so long as the individual remains in PRP.**

(d) A medical evaluation of the individual as set forth in DOD Directive 5210.42 **(AR 50–5)** (reference (s)).

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

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

(g) Service in the Army, Navy and Air Force Reserve does not constitute active service for PRP purposes.

b. **The Commander, CCF, will make security clearance determinations for nuclear duty positions under AR 50–5 (reference(s)). CCF will forward cases that contain potentially disqualifying information to the unit commander for PRP determination if the subject of the investigation is in a critical nuclear duty position. Where potentially disqualifying information exists, CCF will annotate part III of DA Form 873 (Certificate of Clearance and/or Security Determination) "Dossier review required for critical nuclear duty." If potentially disqualifying information does not exist, CCF will annotate the DA Form 873 "PRP/Surety Considered." If the certifying authority waives the potentially disqualifying information, he or she will annotate the individual's DA Form 3180 (Personnel Screening and Evaluation Record) in accordance with chapter 3, AR 50–5 (reference (s)). In this event, the commander shall not annotate "PRP/Surety Considered" in part III of DA Form 873.**

3–504.1. Chemical Personnel Reliability Program

The Commander, CCF, will make security clearance determinations for chemical duty positions under AR 50–6 (reference (y)).

3–504.2. Automation security

The Commander, CCF, will make security clearance determinations for the Personnel Security and Surety Program (PSSP). CCF will forward cases that contain potentially disqualifying information to the unit commander for PSSP determination if the subject of the investigation is in an ADP position. Where potentially disqualifying information exists, CCF will annotate part II of DA Form 873 "Dossier review required for critical nuclear duty. " If potentially disqualifying information does not exist, CCF will annotate the DA Form 873 "PRP/Surety Considered." (See para 3–614 and app K.) If the automation security officer waives the potentially disqualifying information, the commander will not annotate, "PRP/Surety Considered" in part III of DA Form 873.

3–505. Access to North Atlantic Treaty Organization (NATO) classified information

a. Personnel assigned to NATO staff position requiring access to NATO COSMIC (TOP SECRET), SECRET or CONFIDENTIAL information shall have been the subject of a favorably adjudicated BI (10–year scope), DNACI/NACI, or NAC/ENTNAC, current within 5 years prior to the assignment, in accordance with USSAN Instruction 1–69 **(AR 380–15)** (reference (kk)) and paragraph 3–705, below.

b. 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 final U.S. security clearance based upon the appropriate personnel security investigation (app B) required by paragraphs 3–401 and 3–709 of this regulation.

3–506. Other Special Access programs

Special investigative requirements for Special Access programs not provided for in this paragraph may not be established without the written approval of the Deputy Under Secretary of Defense for Policy.

Section VI
Certain Positions Not Necessarily Requiring Access to Classified Information.

3–600. General

DOD Directive 5200.8 **(AR 190–16)** (reference (t)) outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of property or places under their command. Essential to carrying out this responsibility is a commander's need to protect the command against the action of untrustworthy persons. Normally, the investigative requirements prescribed in this regulation should suffice to enable a commander to determine the trustworthiness of individuals whose duties r equire access to classified information or appointment to positions that are sensitive and do not involve such access. However, there are certain categories of positions or duties which, although not requiring access to classified information, if performed by untrustworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security. The investigative requirements for such positions or duties are detailed in this section.

3–601. Access to restricted areas, sensitive information, or equipment not involving access to classified information

a. Access to restricted areas, sensitive information or equipment **(such as critical COMSEC items)** by DOD military, civilian, or contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or ENTNAC) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate Component agency or activity, **MACOM commander and staff agency heads authorized to request security investigations, or head of DA Staff agency** prior to permitting such access. DOD Components, **MACOM commanders, and heads of DA Staff agencies** shall not request, and shall not direct or permit their contractors to request, security clearances to permit access to areas when access to classified information is not required in the normal course of duties or which should be precluded by appropriate security measures. In determining trustworthiness under this paragraph, the provisions of paragraph 2–200 and appendix I will be utilized.

b. In meeting the requirements of this paragraph, approval shall be obtained from one of the authorities designated in paragraph **F–1**, appendix F of this regulation, **or the DCSINT (DAMI–ClS)** for authority to request NACs on DOD military, civilian, or contractor employees. A justification shall accompany each request and shall detail the reasons why escorted access would not better serve the national security. Requests for investigative requirements beyond a NAC shall be forwarded to the Deputy Under Secretary of Defense for Policy for approval.

c. NAC requests shall (1) be forwarded to DIS in accordance with the provisions of paragraph **C–2**, appendix C, (2) contain a reference to this paragraph on the DD Form 398–2, and (3) list the authority in appendix F who approved the request.

d. Determinations to deny access under the provisions of this paragraph must not be exercised in an arbitrary, capricious, or discriminatory manner and shall be the responsibility of the military or installation commander as provided for in DOD Directive 5200.8 **(AR 190–16)** (reference (t)).

3–602. Nonappropriated Fund employees

a. Each Nonappropriated Fund employee who is employed in a position of trust as designated by an official authorized in paragraph **F–8**, appendix F, shall have been the subject of a NAC completed no longer than 12 months prior to employment or a prior personnel security investigation with no break in Federal service or employment greater than 12 months in accordance with DOD 1401.1–M **(AR 215–5)** (reference (u)). An individual who does not meet established suitability requirements may not be employed without prior approval of the authorizing official. Issuance of a CONFIDENTIAL or SECRET clearance will be based on a DNACI or NAC in accordance with paragraph 3–401.

b. **If a Nonappropriated Fund employee requires a security clearance, the commander of the host installation will request a personnel security clearance from CCF.**

3–603. Customs inspectors

DOD employees appointed as customs inspectors, under waivers approved in accordance with DOD 5030.49–R **(AR 190–41)** (reference (v)), shall have undergone a favorably adjudicated NAC completed within the past 5 years unless there has been a break in DOD employment greater than 1 year, in which case a current NAC is required.

3–604. Red Cross/United Service Organizations personnel

a. A favorably adjudicated NAC shall be accomplished on Red Cross or United Service Organizations personnel as a prerequisite for assignment with the Armed Forces overseas (DOD Directive 5210.25 **(AR 380–49)** (reference (w)). **Employees who are not U.S. citizens shall have been the subject of a BI, completed with favorable results, before being nominated for assignment with Army elements overseas.**

b. **A completed personal security questionaire (PSQ) (DD Form 398 or DD Form 398–2) shall be forwarded to the Defense Industrial Security Clearance Office (DISCO), DIS, P.O. Box 2499, Columbus, OH 43216, for initiation of the BI or NAC in accordance with the provisions of DOD Directive 5220.6 (AR 380–49) (reference (c)).**

c. **If a Red Cross or USO employee requires a personnel security clearance, the commander of the host installation will request the appropriate clearance from the Commander, CCF. The request for clearance will include a copy of the favorable employment determination by DISCO.**

3–605. Officials authorized to issue security clearances

Any person authorized to adjudicate personnel security clearances shall have been the subject of a favorably adjudicated BI.

3–605.1. Officials authorized to grant access to SCI

Any person authorized to adjudicate SCI access eligibility will have been the subject of a favorably completed SBI.

3–606. Personnel security clearance adjudication officials

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

3–607. Persons requiring DOD building passes

Pursuant to DOD Directive 5210.46 **(AR 380–4)** (reference (x)), each person determined by the designated authorities of the Components concerned as having an official need for access to DOD buildings in the National Capital Region shall be the subject of a favorably adjudicated NAC prior to issuance of a DOD building pass. Conduct of a BI for this purpose is prohibited unless approved in advance by ODUSD(P).

3–608. Foreign national employees overseas not requiring access to classified information

Foreign nationals employed by DOD organizations overseas, whose duties do not require access to classified information, shall be the subject of the following record checks, initiated by the appropriate Military Department investigative organization consistent with paragraph 2–404, prior to employment:

a. 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;

b. DCII; and

c. FBI–HQ/ID (where information exists regarding residence by the foreign national in the United States for 1 year or more since age 18).

3–609. Special agents and investigative support personnel

Special agents and those noninvestigative personnel assigned to investigative agencies whose official duties require continuous access to complete investigative files and material require an SBI.

3–610. Persons requiring access to chemical agents

Personnel whose duties involve access to or security of chemical agents shall be screened initially for suitability and reliability and shall be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required. At a minimum, all such personnel shall have had a favorably adjudicated NAC completed within the last 5 years prior to assignment in accordance with the provisions of DOD Directive 5210.65. **(AR 50–6)** (reference (y)).

3–611. Education and orientation personnel

Persons selected for duties in connection with programs involving the education and orientation of military personnel shall have been

the subject of a favorably adjudicated NAC prior to such assignment. This does not include teachers/administrators associated with university extension courses conducted on military installations in the United States. Non–U.S. citizens from a country listed in appendix H shall be required to undergo a BI if they are employed in a position covered by this paragraph. **Investigations for military service or civilian employment with a DOD Component satisfy the investigation requirement.**

3–612. Contract guards

Any person performing contract guard functions shall have been the subject of a favorably adjudicated NAC **by DISCO** prior to such assignment **to any security duties and in accordance with AR 190–56 (reference (qq)).**

3–613. Transportation of arms, ammunition and explosives (AA&E)

Any DOD military, civilian or contract employee (including commercial carrier) operating a vehicle or providing security to a vehicle transporting Category I, II, or CONFIDENTIAL AA&E shall have been the subject of a favorably adjudicated NAC or ENTNAC. **Results of the completed NAC or ENTNAC shall be returned to Commander, Military Traffic Management Command (MTMC), ATTN: MT–SS, Room 403, 5611 Columbia Pike, Falls Church, VA 22041–5050, for adjudication.**

3–614. Personnel occupying information systems positions designated ADP–I, ADP–II, and ADP–III

DOD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with app K) and investigated as follows:

Table 1

ADP–I:	BI/SBI
ADP–II:	DNACI/NACI
ADP–III:	NAC/ENTNAC/NACI

Foreign nationals may be assigned to ADP–I and ADP–II positions only by an authority designated in paragraph F–2, appendix F, and paragraph 2–100. Those personnel falling in the above categories who require access to classified information will, of course, be subject to appropriate investigative scope contained in paragraph 3–401, above.

3–615. Others

Requests for approval to conduct an investigation of other personnel not provided for in paragraphs 3–601 through 3–614, above, considered to fall within the general provisions of paragraph 3–600, above, shall be submitted, detailing the justification thereof, for approval **through the DCSINT (DAMI–CIS)** to the Deputy Under Secretary of Defense for Policy. Approval of such requests shall be contingent upon an assurance that appropriate review procedures exist and that adverse determinations will be made at no lower than major command level.

Section VII
Reinvestigation

3–700. General

DOD policy prohibits unauthorized and unnecessary investigations. There are, however, certain situations and requirements that necessitate reinvestigation of an individual who has already been investigated under the provisions of this regulation. It is the policy to limit reinvestigation of individuals to the scope contained in paragraph **B**–5, appendix B, to meet overall security requirements. Reinvestigation, generally, is authorized only as follows:

a. To prove or disprove an allegation relating to the criteria set forth in paragraph 2–200 of this regulation with respect to an individual holding a security clearance or assigned to a position that requires a trustworthiness determination;

b. To meet the periodic reinvestigation requirements of this regulation with respect to those security programs enumerated below; and

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

d. **Reinvestigation will not be requested if the subject is within 12 months of retirement.**

3–701. Allegations related to disqualification

Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the disqualification criteria outlined in paragraph 2–200 that could have an adverse impact on an individual's security status, a special investigative inquiry (SII), psychiatric, drug, or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative subject and the subject fails to furnish the required data, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with paragraph 8–201 of this regulation.

3–702. Access to sensitive compartmented information (SCI)

Each individual having current access to SCI shall be the subject of a PR conducted on a 5–year recurring basis scoped as set forth in paragraph **B**–5, appendix B.

3–703. Critical–sensitive positions

Each DOD civilian employee occupying a critical–sensitive position shall be the subject of a PR conducted on a 5–year recurring basis scoped as set forth in paragraph **B**–5, appendix B.

3–703.1. Critical military duties

All military personnel with a military occupational speciality (MOS) or specialty classification under AR 611–101 (reference (zz)), AR 611–112 (reference (aaa)), or AR 611–201 (reference (bbb)) that requires eligibility for SCI, regardless of access level, shall be the subject of a PR on a 5–year recurring basis as set forth in paragraph B–5, appendix B. So will military personnel with duties that fall under any of the following criteria:

a. **Access to TOP SECRET information.**

b. **Development or approval of plans, policies, or programs that affect the overall operations of the DOD or a Component.**

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

d. **Investigative and certain support duties, adjudication of personnel security clearances or access authorizations, or making personnel security determinations.**

e. **Fiduciary, public contact, or other duties demanding the highest degree of public trust.**

f. **Duties falling under Special Access programs (excluding controlled nuclear duty positions).**

g. **Category I ADP positions.**

h. **Any other position so designated by the Secretary of the Army (SA) or designee.**

3–704. Presidential support duties

Each individual assigned Presidential support duties shall be the subject of a PR conducted on a 5–year recurring basis scoped as set forth in paragraph **B**–5, appendix B.

3–705. NATO staff

Each individual assigned to a NATO staff position requiring a COSMIC clearance shall be the subject of a PR conducted on a 5–year recurring basis scoped as set forth in paragraph **B**–5, appendix B. Those assigned to a NATO staff position requiring a NATO SECRET clearance shall be the subject of a new NAC conducted on a 5–year recurring basis.

3–706. Extraordinarily sensitive duties

In extremely limited instances, extraordinary national security implications associated with certain SCI duties may require very special compartmentation and other special security measures. In such instances, a Component SOIC **or the DCSINT** may, with the approval of the Deputy Under Secretary of Defense for Policy, request PRs at intervals of less than 5 years as outlined in paragraph **B**–5, appendix B. Such requests shall include full justification and a recommendation as to the desired frequency. In reviewing such requests, the Deputy Under Secretary of Defense for Policy shall give due consideration to:

a. The potential damage that might result from the individual's defection or abduction.

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

3–707. Foreign nationals employed by DOD organizations overseas

Foreign nationals employed by DOD organizations overseas who have been granted a "limited access authorization" pursuant to paragraph 3–403 shall be the subject of a PR, as set forth in paragraph **B**–5, appendix B, conducted under the auspices of DIS by the appropriate military department or other U.S. Government investigative agency consistent with paragraph 2–404 and appendix J of this regulation.

3–708. Persons accessing very sensitive information classified SECRET

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

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

(1) Jeopardize human life or safety.

(2) Result in the loss of unique or uniquely productive intelligence sources or methods vital to U.S. security.

(3) Compromise technologies, plans, or procedures vital to the strategic advantage of the United States.

c. Each individual accessing very sensitive SECRET information who has been designated by an authority listed in paragraph **F–1**, appendix F as requiring periodic reinvestigation, shall be the subject of a PR conducted on a 5–year recurring basis scoped as stated in paragraph **B**–5, appendix B.

3–709. Access to TOP SECRET information

Each individual having current access to TOP SECRET information shall be the subject of a PR conducted on a 5–year recurring basis scoped as outlined in paragraph **B**–5, appendix B.

3–710. Personnel occupying computer positions designated ADP–I

All DOD military, civilian, consultant, and contractor personnel occupying computer positions designated ADP–I shall be the subject of a PR conducted on a 5–year recurring basis as set forth in paragraph **B**–5, appendix B.

3–711. Critical nuclear duty positions

All DA military (including those with an MOS that requires eligibility for critical nuclear duties), civilian, and contractor personnel occupying critical nuclear duty positions in accordance with AR 50–5 (reference(s)) shall be the subject of a PR conducted on a 5– year recurring basis as set forth in paragraph B–5, appendix B.

Section VIII
Authority to Waive Investigative Requirements

3–800. Authorized officials

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

3–801. Combat operations, DA–directed mobilization

Under combat conditions, authorities listed in paragraph F–7, appendix F, may waive such provisions of this regulation as are operationally necessary and warranted by the circumstances. Under mobilization or similar conditions and mobilization exercises, prior approval to waive requirements ofthis regulation must be obtained from the DCSINT (DAMI–CIS). This authority may be redelegated to commanders of subordinate elements to expedite security clearance actions. Such redelegation will not be made to echelons below that at which the Military Personnel Records Jacket (MPRJ) is maintained.Investigative prerequisites waived under the authority of this paragraph will be complied with as soon as the situation permits.

Chapter 4
Reciprocal Acceptance of Prior Investigations and Personnel Security Determinations

4–100. General

Previously conducted investigations and previously rendered personnel security determinations shall be accepted within DOD in accordance with the policy set forth below.

4–101. Prior investigations conducted by DOD investigative organizations

As long as there is no break in military service/civilian employment greater than 12 months, any previous personnel security investigation conducted by DOD investigative organizations that essentially is equivalent in scope to an investigation required by this regulation will be accepted without requesting additional investigation. There is no time limitation as to the acceptability of such investigations, subject to the provisions of paragraphs 2–307 and 4–102*b* of this regulation.

4–102. Prior personnel security determinations made by DOD authorities

a. Adjudicative determinations for appointment in sensitive positions, assignment to sensitive duties or access to classified information (including those pertaining to SCI) made by designated DOD authorities will be mutually and reciprocally accepted by all DOD Components without requiring additional investigation, unless there has been a break in the individual's military service/civilian employment of greater than 12 months or unless derogatory information that occurred subsequent to the last prior security determination becomes known. A check of the DCII should be conducted to accomplish this task.

b. Whenever a valid DOD security clearance or Special Access

authorization (including one pertaining to SCI) is on record, Components shall not request DIS or other DOD investigative organizations to forward prior investigative files for review unless:

(1) Significant derogatory information or investigation completed subsequent to the date of last clearance or Special Access authorization is known to the requester; or

(2) The individual concerned is being considered for a higher level clearance (e.g., SECRET or TOP SECRET) or the individual does not have a Special Access authorization and is being considered for one; or

(3) There has been a break in the individual's military service/civilian employment of greater than 12 months subsequent to the issuance of a prior clearance; or

(4) The most recent SCI access authorization of the individual concerned was based on a waiver.

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

d. All requests for non–DOD investigative files, authorized under the criteria prescribed by paragraphs *a*, *b*(l), (2), (3), and (4) and *c*, above, shall be:

(1) Submitted on DD Form 398–2 to DIS;

(2) Annotated as a "Single Agency Check" of whichever agency or agencies developed the investigative file or to obtain the check of a single national agency.

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

f. Whenever a civilian or military member transfers from one DOD activity to another **(or from one Army organization to another),** the losing organization is responsible for advising the gaining organization of any pending action to suspend, deny, or revoke the individual's security clearance as well as any adverse information **(or disqualifying information, i.e., marriage to a foreign national)** 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.

4–103. Investigations conducted and clearances granted by other agencies of the Federal Government

a. Whenever a prior investigation or personnel security determination (including clearance for access to information classified under Executive Order 12356 (reference (j)) of another agency of the Federal Government meets the investigative scope and standards of this regulation, such investigation or clearance may be accepted for the investigative or clearance purposes of this regulation, provided that the employment with the Federal agency concerned has been continuous and there has been no break longer than 12 months since completion of the prior investigation, and further provided that inquiry with the agency discloses no reason why the clearance should not be accepted. If it is determined that the prior investigation does not meet the provisions of this paragraph, supplemental investigation shall be requested.

b. A NACI conducted by OPM **is of greater scope than a NAC or DNACI, and** shall be accepted and considered equivalent to a DNACI for the purposes of this regulation.

c. Department of Defense policy on reciprocal acceptance of clearances with the Nuclear Regulatory Commission and the Department of Energy is set forth in DOD Directive 5210.2 **(AR 380–150)** (reference (z)).

d. **When a DA organization must authorize access to classified information in its custody to a member of another service or agency who has not been cleared or who needs a higher degree of clearance, the parent service or agency will be asked to grant the clearance.**

e. **If it is not in the best interests of the national security to permit the person access to classified defense information in Army custody, or if the person is denied the required clearance, the commander will reassign the person to nonsensitive duties or, if appropriate, revoke the detail or assignment and advise the parent Service or agency of the reasons. The parent Service or agency is responsible for initiating security proceedings and denying or revoking a security clearance.**

f. **The Commander, CCF, is responsible for granting, revoking, or denying security clearances for Army personnel who are assigned or detailed to other Services, Defense Agencies, and the Unified and Specified Commands.**

Chapter 5
Requesting Personnel Security Investigations

5–100. General

Requests for personnel security investigations shall be limited to those required to accomplish the Defense mission. Such requests shall be submitted only by the authorities designated in paragraph 5–101 below. These authorities shall be held responsible for determining if persons under their jurisdiction require a personnel security investigation. Proper planning must be effected to ensure that investigative requests are submitted sufficiently in advance to allow completion of the investigation before the time it is needed to grant the required clearance or otherwise make the necessary personnel security determination.

5–101. Authorized requesters

Requests for personnel security investigation shall be accepted only from the requesters designated below:

a. Military Departments

(1) *Army*

(a) **CCF, Fort George G. Meade, MD 20755–5250.**

(b) **DCSINT.**

(c) All activity commanders **designated in paragraph F–7.**

(d) Chiefs of recruiting stations.

(e) **State adjutants general for the ARNG.**

(2) *Navy (including Marine Corps)*

(a) Central Adjudicative Facility.

(b) Commanders and commanding officers of organizations listed on the Standard Navy Distribution List.

(c) Chiefs of recruiting stations.

(3) *Air Force*

(a) Air Force Security Clearance Office.

(b) Assistant Chief of Staff for Intelligence.

(c) All activity commanders.

(d) Chiefs of recruiting stations.

b. Defense Agencies—Directors of Security and activity commanders.

c. Organization of the Joint Chiefs of Staff—Chief, Security Division.

d. Office of the Secretary of Defense—Director for Personnel and Security, Washington Headquarters Services.

e. Commanders of the Unified and Specified Commands or their designees.

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

5–102. Criteria for requesting investigations

Authorized requesters shall use the tables set forth in appendix D to determine the type of investigation that shall be requested to meet the investigative requirement of the specific position or duty concerned.

5–103. Request procedures

To ensure efficient and effective completion of required investigations, all requests for personnel security investigations shall be prepared and forwarded in accordance with appendix C and the

investigative jurisdictional policies set forth in section IV, chapter 2 of this regulation.

5–104. Priority requests

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

5–105. Personal data provided by the subject of the investigation

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

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

c. Failure to respond within the time limit prescribed by the requesting organization with the required security forms or refusal to provide or permit access to the relevant information required by this regulation shall result in termination of the individual's security clearance or assignment to sensitive duties utilizing the procedures of paragraph 8–201 or further administrative processing of the investigative request.

5–106. Requests for additional information or clarification

When questionable behavior, inconsistencies, or other derogatory information related to the criteria in paragraph 2–200 arise, CCF may request more information or clarification directly from the field commander or the subject (see para 3–701). Such requests include, but are not limited to the following:

a. **Results of command inquiries and investigations; copies of courts–martial proceedings; copies of administrative or disciplinary actions, written reprimands, Articles 15; results of local records file checks or of previous psychiatric or drug and alcohol evaluations; or letters of indebtedness received by the command.**

b. **DD Forms 398, fingerprint cards, and other forms or release statements required to conduct investigations; verification of citizenship of the subject and/or immediate family. Occasionally, to expedite the decisionmaking process, CCF will ask security managers to obtain specific information from the subject, such as current financial status, proof of payment of delinquent debts, or clarification of information listed on DD Form 398 or similar forms.**

c. **Progress and final reports from Alcohol and Drug Abuse Prevention and Control Program (ADAPCP) officials on alcohol and drug rehabilitation treatment. Such reports will include history and extent of substance abuse, diagnosis, attitude toward treatment, results of treatment, and immediate and long–term prognosis. CCF will request a current alcohol or drug evaluation when incidents of alcohol or drug abuse are reported and the subject has not been referred for drug and/or alcohol treatment; more than 1 year has passed since treatment occurred, or it occurred during a previous assignment and results are not available; or there was an indication of substance abuse after completion of treatment. A physician or mental health clinician trained in the alcohol and drug rehabilitation field, who is employed by or under contract to the U.S. military or U.S. Government, will conduct the evaluation. The purpose of the evaluation is to assess the subject's ability to refrain from abuse and to obtain an opinion on the potential impact upon the subject's judgment and reliability in protecting classified information and material.**

d. **Information from medical records that indicates mental disorder or emotional instability or results of any psychiatric or mental health evaluation or treatment for a mental condition. When any information indicates a history of mental or nervous disorder or reported behavior appears to be abnormal, indicating impaired judgment, reliability, or maturity, CCF will request a mental health evaluation to determine whether or not any defect in judgment or reliability or any serious behavior disorder exists. A board– certified or board–eligible psychiatrist or licensed or certified clinical psychologist who is employed by or under contract to the U.S. military or U.S. Government will conduct mental health evaluations for security clearance purposes. The evaluation report should outline the methods used in the evaluation (for example, psychological testing and clinical interviews), include a narrative case history, assess the results of any psychological tests, and include a diagnosis under DSM III (see note) or state that no diagnosis exists. The report should include a prognosis and indicate what effect the diagnosed condition has on judgment, reliability, and stability, and describe any characteristics in a normal or stressful situation. If the individual's condition is under control through treatment or medication, the report should indicate what could happen if the individual did not comply with treatment and what likelihood exists of failure to comply. If appropriate, the report should indicate an estimated time or condition that could cause a favorable change.**

Note: American Psychiatric Association: Diagnostic and Statistical Manual of Mental Disorders, Third Edition, Wash, DC: APA, 1980.

e. **It is imperative, in the interests of national security, that the commander and the subject of the case respond promptly to CCF's request for information. Failure to respond to requests for information required by CCF for personnel security clearance determinations within the prescribed time shall result in CCF directing suspension of the individual's access to classified information or termination of action to process request for security clearance. Continued failure to respond to CCF's request for information shall result in action to terminate the individual's security clearance utilizing the procedures of paragraph 8–201.**

5–107. Grounds for denial

If information developed by the command indicates the existence, current or past, of any mental or nervous disorder or emotional instability, a request for a PSI will not be submitted and interim clearance will not be granted. Clearance can be

granted only if competent medical authority, as defined above, certifies that the disorder or instability has been overcome or will not cause a defect in the person's judgment or reliability.

5–108. Requesting NACIs from OPM

A NACI will be submitted to OPM according to OPM instructions. Block H of the agency use block of Standard Form 86 will show the employing agency's security office identification (SOI) number where OPM will forward the results of the NACI. The Security Manager will coordinate with the appropriate civilian personnel office to determine eligibility for employment prior to requesting a security clearance determination from CCF.

a. **If the NACI is completely favorable, the Security Manager may attest to that fact in the "Remarks" block of DA Form 5247–R. If the NACI contains unfavorable information, a copy of the entire NACI will be submitted to the CCF with the request for security clearance.**

b. **If the NACI contains other than minor unfavorable information, an interim clearance is not authorized and DA Form 5247–R will indicate that a favorable employment determination was made.**

c. **If a clearance is not immediately required, the NACI results may be maintained by the Security Manager as long as the person is employed and may be transferred within the DOD.**

Chapter 6
Adjudication

6–100. General

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

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

c. 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.

d. 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.

6–101. Central adjudication

a. To ensure uniform application of the requirement of this regulation and to ensure that DOD personnel security determinations are effected consistent with existing statutes and Executive orders, the head of each Military Department and Defense Agency shall establish a single central adjudication facility for his or her Component. **The CCF, Fort George G. Meade, MD, has been designated as the single central adjudication facility for the DA.** The function of each facility **or the CCF** shall be limited to evaluating personnel security investigations and making personnel security determinations. The Chief of each central adjudication facility **or Commander, CCF,** shall have the authority to act on behalf of the head of the Component **or the SA** with respect to personnel security determinations. All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this regulation shall be reviewed and evaluated by personnel security specialists specifically designated by the head of the Component concerned, or designee, **or by the SA or the DCSINT.**

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

(1) *BI/SBI/PR/ENAC/SII:*

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

(b) Unfavorable: Investigations that are not completely favorable shall undergo at least two levels of review by adjudicative officials, the second of which must be at the civilian grade of GS–11/12 or the military rank of O–4. When an unfavorable administrative action is contemplated under paragraph 8–201, the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS–13/14 or the military rank of O–5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS–14/15 or the military rank of O–6.

(2) *NACI/DNACI/NAC/ENTNAC:*

(a) Favorable: A completely favorable investigation may be finally adjudicated after one level of review provided that the decisionmaking authority is at the civilian grade of GS–5/7 or the military rank of O–2.

(b) Unfavorable: Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS–7/9 or the military rank of O–3. When an unfavorable administrative action is contemplated under paragraph 8–201, the letter of intent to deny/revoke must be signed by an adjudicative official at the civilian grade of GS–11/12 or the military rank of O–4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS–13 or the military rank of O–5 or above.

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

6–102. Evaluation of personnel security information

a. The criteria and adjudicative policy to be used in applying the principles at paragraph 6–100, above, are set forth in paragraph 2–200 and appendix I 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:

(1) The nature and seriousness of the conduct;
(2) The circumstances surrounding the conduct;
(3) The frequency and recency of the conduct;
(4) The age of the individual;
(5) The voluntariness of participation; and
(6) The absence or presence of rehabilitation.

b. 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 I. Adjudication policy for access to SCI is contained in DCID 1/14.

6–103. Adjudicative record

a. Each clearance/access determination, whether favorable or unfavorable, shall be entered **by the Commander, CCF,** into the Defense Central Security Index (DCSI), a sub–element of the Defense Central Index of Investigations (DCII). (Operational details regarding implementation of the DCSI shall be implemented in a forthcoming change to this regulation.)

b. The rationale underlying each unfavorable administrative action shall be reduced to writing and is subject to the provisions of DOD Directive 5400.7 **(AR 340–17)** (reference (aa)) and DOD Directive 5400.11 **(AR 340–21)** (reference (bb)).

6–104. Reporting results of security or suitability determinations for civilian employees

CCF will forward a copy of the initial BI or SBI of civilian employees, conducted by DIS, to the Security Manager of the employing command after making a security clearance determination. This will allow the employing command to determine employment eligibility and notify OPM. Employing activities will forward OFI Form 79A to report security or suitability determinations based on results of BI/SBI to: OPM–FIPC, ATTN: OFI 79A, Boyers, PA 16018–0618, within 30 days after final determination.

Chapter 7
Issuing Clearance and Granting Access

7–100. General

a. The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph 8–201.

b. Only the authorities designated in paragraph **F–1**, appendix F, are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization, **to include CCF,** may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in paragraph 8–102 of this regulation are complied with.

c. All commanders and heads of DOD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this regulation.

7–101. Issuing clearance

a. Authorities designated in paragraph **F–1**, appendix F, shall record the issuance, denial or revocation of a personnel security clearance in the DSCI (see para 6–103, above). A record of the clearance issued shall also be recorded in an individual's personnel/security file or official personnel folder, as appropriate. **The Commander, CCF, will forward DA Form 873 to the command security manager for inclusion in the OPF or in the MPRJ in accordance with AR 640–10 (reference (ddd)). The DA Form 873 will not be removed except to make a copy, correct an administrative error, when a more recent clearance certificate is issued by CCF, to suspend access, or to comply with a direction of CCF.**

b. A personnel security clearance remains valid until (1) the individual is separated from the Armed Forces, (2) separated from DOD civilian employment, (3) has no further official relationship with DOD **or other Federal agencies,** (4) official action has been taken to deny, revoke or suspend the clearance or access, or (5) regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties. If an individual resumes the original status of (1), (2), (3), or (5) above, no single break in the individual's relationship with DOD exists greater than 12 months, and/or the need for regular access to classified information at or below the previous level recurs, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

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

d. When a Defense Agency, to include OJCS, initiates an SBI (or PR) for access to SCI on a military member, DIS will return the completed investigation to the appropriate Military Department adjudicative authority in accordance with paragraph *c*, above, for issuance (or reissuance) of the TOP SECRET clearance. Following the issuance of the security clearance, the military adjudicative authority will forward the investigative file to the Defense Agency identified in the "Return Results To" block of the DD Form 1879. The receiving agency will then forward the completed SBI on to DIA for the SCI adjudication in accordance with DCID 1/14 **(reference (b))**.

e. The interim clearance **will be recorded on DA Form 873 and**shall be recorded in the DCSI by the parent DOD Component **in accordance with paragraph 6–103** in the same manner as a final clearance. **If a final clearance has not been received within 150 days, commanders will submit DA Form 5247–R (Request for Security Determination) to CDR, CCF (PCCF–M), as a tracer action and extend the interim period for an additional 180 days. If the DCII reveals existence of unevaluated derogatory information, CCF will advise requester that interim clearance is not authorized.**

f. **Requests for investigation for security clearances (DD Form 1879 and DD Form 398–2) forwarded to DIS do not require submission of DA Form 5247–R to CCF. DIS will forward the completed investigation to CCF, who will make a clearance determination and inform the requester. If a clearance determination is not received in 150 days, the requester may trace the action by forwarding DA Form 5247–R to CCF. Commands should forward DA Form 5247–R on newly arrived personnel in their command if the personnel file or the individual indicates that an investigation was initiated at the former command. This will allow CCF to forward the clearance determination to the current commander.**

g. **CCF will forward DA Form 873 to the command whose unit identification code (UIC) appears on the DA Form 5247–R, DD Form 1879, or DD Form 398–2, if the UIC is documented in**

CCF'S data base. The UIC is used by CCF to add the requester's mailing address to the DA Form 873. Action to add, delete, or correct a UIC or associated address should be forwarded to Commander, CCF (PCCF–S). Commands may also request that a higher command, "THRU" UIC, be associated with any of their subordinate command UICs. This will allow CCF to forward the DA Form 873 addressed through the higher headquarters to the subordinate commander.

7–102. Granting access

a. Access to classified information shall be granted to persons whose official duties require such access, and who have the appropriate personnel security clearance. **CCF normally grants the highest level of clearance authorized by the personnel security investigation on record.** Access determinations (other than for Special Access programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

b. In the absence of derogatory information on the individual concerned, DOD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DOD authority authorized by this regulation to issue personnel security clearances, as the basis for granting access, when access is required, without requesting additional investigation or investigative files. **For Army–affiliated personnel, this determination is documented by a DA Form 873 in the personnel file. A DA Form 873, as well as clearance certificates issued by other DOD Components, will be honored provided—**

(1) **There has been no break in Federal service exceeding 12 months since the investigation date; and**

(2) **A check of local records discloses no unfavorable information.**

c. The access level of cleared individuals will also be entered into the DCSI **by the Commander, CCF,** along with clearance eligibility status, as systems are developed and adopted which make such actions feasible.

d. **Once the Commander, CCF, has granted a person's security clearance, special access for NATO, SIOP–ESI, or other programs will be granted by the commander responsible for their control under appropriate regulations. The Commander, CCF, will make all eligibility determinations for SCI access.**

e. **DA Form 5247–R, with a copy of the clearance documentation, will be forwarded to CDR, CCF (PCCF–M), when accepting an Army clearance granted prior to CCF's assumption of clearance authority or by another DOD Component or Federal agency. In these cases, access to classified information need not be delayed pending receipt of a DA Form 873. Access may be granted and continued provided local file checks are favorable. Forwarding is not necessary if DA Form 873 is annotated, "Project Top Feed Completed."**

7–103. Administrative withdrawal

As set forth in paragraph 7–101*b*, above, the personnel security clearance and access eligibility must be withdrawn when the events described therein occur. When regular access to a prescribed level of classified information is no longer required in the normal course of an individual's duties, the previously authorized access eligibility level must be administratively downgraded or withdrawn, as appropriate. **Access based on an investigation completed over 5 years ago will be limited to no higher than SECRET unless a request for periodic reinvestigation was forwarded to DIS prior to the 5–year anniversary date of the previous investigation.**

Chapter 8
Unfavorable Administrative Actions

Section I
Requirements

8–100. General

For purposes of this regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at paragraph 1–301, and any unfavorable personnel security determination, as defined at paragraph 1–329. This chapter is intended only to provide guidance for the internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

8–101. Referral for action

a. Whenever derogatory information relating to the criteria and policy set forth in paragraph 2–200 and appendix I of this regulation is developed or otherwise becomes available to any DOD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall ensure that the parent Component of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto **by forwarding DA Form 5248–R (Report of Unfavorable Information for Security Determination) to the Commander, CCF (PCCF–M).** However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph 8–201, below, if such action is warranted and supportable by the criteria and policy contained in paragraph 2–200 and appendix I. No unfavorable administrative action as defined in paragraphs 1–328 and 329 may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in paragraph 8–201, below, or, in the case of SCI, Annex B, DCID 1/14 (reference (l)).

b. The Director, DIS, shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other than through DOD command or industrial organization channels. Such access shall include utilization of the DOD Inspector General "hotline" to receive such reports for appropriate followup by DIS. DOD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DOD Components will augment the system when and where necessary. Heads of DOD Components will be notified immediately to take action if appropriate.

(1) **When the commander learns of credible derogatory information on a member of his or her command that falls within the scope of paragraph 2–200, the commander will immediately forward DA Form 5248–R to the Commander, CCF.**

(2) **DA Form 5248–R will be submitted in a timely manner. At a minimum, initial reports will indicate the details of the credible derogatory information and actions being taken by the commander or appropriate authorities (for example, conducting an inquiry or investigation) to resolve the incident. Followup reports will be submitted at 90–day intervals if the commander has not taken final action or, for example, the subject is still pending action by civil court. At the conclusion of the command action, a final report will be forwarded to CCF indicating the action taken by the commander. The final report must contain results of any local inquiry, investigation, or board action and**

recommendation of the command concerning restoration or revocation of the person's security clearance, if appropriate.

(3) **Commanders will not delay any contemplated personnel action while awaiting final action by CCF. The personnel action should proceed, with CCF being informed of the final action by submission of DA Form 5248–R through established channels.**

(4) **If the personnel file does not indicate the existence of a security clearance, commanders must still report information that falls within the scope of paragraph 2–200, since the person might later require a clearance. Only a final report is required on personnel who do not have a security clearance.**

(5) **SSOs are charged with protecting SCI. If an SSO learns of any derogatory information falling within the scope of paragraph 2–200 concerning any person under the SSO's security cognizance, the SSO will immediately inform the commander. The failure of a commander to forward a DA Form 5248–R to CCF, when derogatory information has been developed on SCI indoctrinated individuals, should be brought to the attention of the individual's security manager and the Senior Intelligence Officer (SIO).**

8–102. Suspension

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

a. **When a commander learns of significant derogatory information falling within the scope of paragraph 2–200, in addition to the reporting requirements of 8–101 *a* , above, the commander must decide whether or not to suspend the individual's access to classified information. The commander may wish to suspend access on an "informal" basis while gathering information to determine whether or not formal suspension is warranted. After gathering the required data, the commander may decide to restore access. If the commander does not suspend access, CCF will review all available information and, if warranted, advise the commander to suspend access.**

b. **If the commander decides on formal suspension of access, DA Form 873 will be removed from individual's personnel file and attached to DA Form 5248–R reporting the suspension to CCF. Once this is done, the commander may not restore access until a final favorable determination by the Commander, CCF, unless ALL the following criteria are met. These following procedures apply to both collateral and SCI access:**

(1) **If the commander determines that the person has been cleared of all charges and that the alleged offense or disqualifying information has been disproved or found groundless, and the commander is completely convinced that no element of risk remains, the commander may restore interim access in the name of the Commander, CCF. The commander will notify CCF of this action. Access will not normally be restored in cases where factors such as dismissal of charges, acquittal because of legal technicalities, plea bargaining, or absence of a speedy trial are involved. These factors cannot be construed as a clearing of all charges.**

(2) **When the commander is considering suspending or has suspended a person's access because of a suspected or actual psychological problem, the commander may elect to retain the person in status or reinstate access if the following conditions are met:**

(a) **A current medical evaluation indicates the condition was a one–time occurrence.**

(b) **The condition has no lasting effects that would affect the person's judgment.**

(c) **There is no requirement for further medical consultation relating to the condition.**

(d) **The examining physician recommends the person be returned to full duty status.**

(e) **The person exhibits no unacceptable behavior after the favorable medical evaluation.**

(f) **The commander firmly believes the person does not pose a risk to the security of classified information.**

(3) **If the commander has any doubts concerning the person's current acceptability for access, even though the above provisions have been met, the case will be referred to CCF. Only the Commander, CCF, may reinstate access in cases where the person attempted suicide.**

c. **The commander will ensure that the SSO is expeditiously notified of any information within the scope of paragraph 2–200 if the person is indoctrinated for SCI. This notification is especially critical if the commander suspends access.**

d. **A commander who suspends access to classified information will ensure that the suspension is documented in the Field Determined Personnel Security Status data field of the Standard Installation/Division Personnel System personnel file.**

8–103. Final unfavorable administrative actions

The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in appendix F, except that the authority to terminate the employment of a civilian employee of a Military Department or Defense Agency is vested solely in the head of the DOD Component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DOD Components, on the basis of criteria listed in paragraphs 2–200, *a* through *f* , shall be coordinated with the Deputy Under Secretary of Defense for Policy prior to final action by the head of the DOD Component. DOD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the Military Departments. However, actions contemplated in this regard shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of a security clearance, or access to classified information on or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this regulation.

Section II
Procedures

8–200. General

No final personnel security determination shall be made on a member of the Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in 8–201 below, when such determination results in an unfavorable administrative action (see para 8–100). As an exception, Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by DOD Directive 5210.25 **(AR 380–49)**(reference (w)).

8–201. 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 given:

a. A written statement of the reasons why the unfavorable administrative action is being taken. The statement shall be as comprehensive and detailed as the protection of sources afforded confidentiality under the provisions of the Privacy Act of 1974 (5 U.S.C. 552a) (reference (m)) and national security permit. Prior to issuing a statement of reasons to a civilian employee for suspension

or removal action, the issuing authority must comply with the provisions of Federal Personnel Manual, chapter 732, subchapter 1, paragraph 1–6b (reference (cc)). The signature authority must be as provided for in paragraph 6–101*b*(1)(b) and 6–101*b*(2)(b).

(1) **The Commander, CCF, is the DA authority for denial and/or revocation of security clearances and/or SCI access eligibility. The Commander, CCF, may delegate this authority to those individuals outlined in paragraph 6–101 *b*.**

(2) **When CCF receives credible derogatory information and denial or revocation of a security clearance and/or SCI access eligibility is considered appropriate, CCF will forward a letter of intent through the command security manager to the individual. This LOI will outline the derogatory information and explain the proposed action. It will offer the person a chance to reply in writing with an explanation, rebuttal, or mitigation for the incidents.**

(3) **The LOI will direct suspension of access to classified information. If the LOI addresses SCI access only, access to collateral information may continue.**

(4) **If the person needs access to classified information in order to prepare a response to the LOI, CCF may authorize limited access for that specific purpose.**

(5) **When a commander receives an LOI concerning a person who is no longer assigned to the command, one of the following actions will be taken:**

(a) **If the person is transferred, endorse the LOI to the gaining command and forward an information copy of the endorsement to CCF (PCCF–M).**

(b) **If the person has been released from active duty and has a Reserve obligation, forward the LOI to the U.S. Army Reserve Personnel Center, ATTN: DARP–SPI, St. Louis, MO 63132–5200. Forward an information copy of the endorsement to CCF (PCCF–M).**

(c) **If the person has been discharged from military service with no Reserve obligation, endorse the LOI to CCF (PCCF–M), attaching a copy of the discharge orders.**

(6) **The Commander, CCF, may waive the due process requirements of this chapter when a person is incarcerated by military or civilian authorities on conviction of a criminal offense, or when a person is dropped from the rolls as a deserter. In such instances, the commander will take the following actions immediately:**

(a) **Withdraw the DA Form 873 from the person's MPRJ or OPF and stamp or print across the face, "Revoked by authority of Commander, CCF—deserted (date)" or "Revoked by authority of Commander, CCF—incarcerated as a result of civil conviction or court–martial (date)," as appropriate for military and civilian personnel. Forward the DA Form 873 and DA Form 5248 explaining the circumstances to the Commander, CCF (PCCF–M).**

(b) **If the MPRJ or OPF does not contain a DA Form 873, forward DA Form 5248–R, explaining the circumstances, to the Commander, CCF (PCCF–M).**

b. An opportunity to reply in writing to such authority as the head of the Component concerned may designate.

(1) **The commander will ensure that the person acknowledges receipt of the LOI by signing and dating the form letter enclosed with the LOI. The person will indicate his or her intention of submitting a rebuttal. The form letter will be forwarded immediately to CCF.**

(2) **The commander will ensure that the person is counseled as to the seriousness of CCF's contemplated action and will offer advice and assistance needed in forming a reply. The person may seek advice from The Judge Advocate General or other lawyer (at his or her own expense) and may request a copy of the investigative files under the provisions of the Privacy Act. Privacy requests must be forwarded to the Chief, Freedom of Information/Privacy Office, U.S. Army Intelligence and Security Command, ATTN: IACSF–FI, Fort George G. Meade, MD 20755–5995. If other than Army investigative records repository files exist, the Freedom of Information (FOI)/Privacy Office will refer the request to the appropriate repository. The individual must provide full name (including aliases), SSN, and date and place of birth. The person's signature must be notarized by a commissioned officer. If the person requires an extension of the 60–day suspension, the command security manager should forward a request, with justification, to the Commander, CCF (PCCF–M). An expected completion date will be provided.**

(3) **The person's response must address each issue raised in CCF's LOI. Any written documentation may be forwarded. Letters of recommendation from supervisory personnel may be attached to the response.**

(4) **The person will forward the response to CCF through the representative of the commander who provided the LOI. The LOI must be endorsed by at least one commander. The commander should recommend whether the person's clearance should be denied, revoked, or restored. The commander should provide a rationale, addressing the issues outlined in the LOI. Responses to LOIs that do not include the commander's recommendation will be returned with a request for comments.**

c. A written response to any submission under subparagraph b, stating the final reasons therefor, which shall be as specific as privacy and national security considerations permit. The signature authority must be as provided for in paragraphs 6–101*b*(1)(b) and 6–101*b*(2)(b). Such response shall be as prompt as individual circumstances permit, not to exceed 60 days from the date of receipt of the appeal submitted under subparagraph *b*, above, provided no additional investigative action is necessary. If a final response cannot be completed within the timeframe 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, in any case, exceed a total of 90 days from the date of receipt of the appeal under subparagraph *b*.

(1) **CCF's decision is considered final. This decision will be forwarded through the command security office to the individual.**

(2) **In accordance with AR 600–37 (reference (vv)), CCF must provide unfavorable information developed during the PSI to both the DA Suitability Evaluation Board (DASEB) and the appropriate TAPA, Army Reserve Personnel Center, or Guard Personnel Center personnel management office (PMO) on all senior enlisted (E–6 and above), commissioned, or warrant officer personnel. Specifically included is any information that results in denial or revocation of a security clearance. A copy of CCF's LOI, the person's response, and CCF's final letter will be forwarded. The regulation does not exclude providing other significant unfavorable information that does not in itself result in an adverse decision. The DASEB determines which information is retained in a person's official military personnel file (OMPF). The fact that the information is being forwarded to the DASEB or PMO will be documented in CCF's final letter of determination.**

d. An opportunity to appeal to a higher level of authority designated by the Component concerned.

(1) **CCF's final letter of determination will state that if the person intends to appeal, the appeal must be submitted to HQDA (DAMI–CIS) within 60 days from receipt of the letter. The commander will ensure that the person acknowledges receipt of the letter by signing and dating the form letter enclosed with it. If the person does not submit an appeal, the case will be closed, no further appeal will be authorized, and due process will be complete. Requests for extension of time to appeal will be approved only in exceptional cases; they must be in writing, endorsed by the immediate commander, and submitted to HQDA (DAMI–CIS) for approval. Only the subject of the denial or revocation may initiate the appeal. The appeal will be addressed, at a minimum, through the immediate commander. The commander must comment on the action and recommend for or against reinstatement of the security clearance and/or SCI access eligibility. The commander's comments should address the**

issues in the CCF LOI. Any appeal will be made solely on the merits as the case stands.

(2) **If, upon review of the appeal, a determination by HQDA (DAMI–CIS) results in continued denial or revocation, no further appeal is authorized.**

8–201.1. Requests for reconsideration

a. **If during the 60 days following receipt of CCF's final letter of determination the subject has additional information in rebuttal or mitigation, he or she should submit it to the Commander, CCF, rather than submitting an appeal to HQDA (DAMI–CIS). DAMI– CIS will forward such information to the CCF Commander. If the CCF review again results in denial or revocation, the person may then appeal to HQDA.**

b. **If after a final determination by the Commander, CCF, or by HQDA (DAMI–CIS), the person files an appeal, CCF will accept no requests for reconsideration based solely on the passage of time as a mitigating factor for at least 1 year from the date of the final letter of determination or the DA appeal decision, whichever was later.**

c. **Any request for reconsideration submitted to the Commander, CCF, in accordance with the provisions of subparagraphs *a* and *b*, above, must outline the reasons for loss of clearance and provide a rationale for favorable action by CCF. The request for reconsideration must be endorsed by the person's commander. The commander should be familiar with the information available to CCF and with CCF's rationale for denial or revocation. The commander should state why the clearance and/or SCI access should be restored. If the person is not able to provide the commander with a copy of CCF's original action, the commander should request a copy of the Army Investigative Records Repository dossier through his or her authorized file requester, normally the installation directorate of security (DSEC)/security manager at separate brigade, division, corps, and major command levels.**

8–201.2. Involuntary separation of military members and DA civilian personnel

As soon as involuntary separation is considered for military members or DA civilian personnel who have had access to SCI, Special Access programs, or other sensitive programs, the local commaner will send the information listed below to HQDA DAMI–CIS), Washington, DC 20310–1051.Elimination action will not be completed until DAMI–CIS acknowledges receipt of this information.

a. **Individual's name, grade, and SSN.**

b. **Date and place of birth.**

c. **Marital status.**

d. **Length of service.**

e. **Reason(s) for proposed involuntary discharge or dismissal.**

f. **Type of discharge or dismissal contemplated.**

g. **Level of access to classified information. Classified details should not be submitted.**

8–202. Exceptions to policy

a. Notwithstanding paragraph 8–201 above or any other provision of this Regulation, nothing in this regulation shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to Section 7532, Title 5, United States Code (reference (pp)). Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph 8–201, above, are not appropriate. Such determination shall be conclusive.

b. **Notification of adverse action need not be given to—**

(1) **Military personnel who have been dropped from the rolls of their organization for absence without authority.**

(2) **Persons who have been convicted of a criminal offense by a civilian court or court–martial and are incarcerated.**

Section III
Reinstatement of Civilian Employees

8–300. General

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

8–301. Reinstatement benefits

A DOD civilian employee whose employment has been suspended or terminated under the provisions of this regulation and who is reinstated or restored to duty under the provisions of Section 3571, Title 5, United States Code (reference (dd)) is entitled to benefits as provided for by Section 3 of Public Law 89–380 (reference (ee)).

Chapter 9
Continuing Security Responsibilities

Section I
Evaluating Continued Security Eligibility

9–100. General

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

9–101. Management responsibility

a. 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 implication of their duties and on their individual responsibilities.

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

9–102. Supervisory responsibility

Security programs shall be established to ensure that supervisory

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

a. In conjunction with **the submission of BIs and SBIs stated in chapter 2, section II, and appendix B, paragraphs B–3 and B–4; and with** the submission of PRs stated in section VII, chapter 3, and paragraph **B–**5, appendix;supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's **initial or** continued eligibility for access to classified information is omitted.

b. If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's **initial or** continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package. "I am aware of no information of the type contained at appendix E, DOD 5200.2–R, **(AR 380–67)** relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information."

c. If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated, and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package: "I am aware of information of the type contained in appendix E, DOD 5200.2–R **(AR 380–67)**, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s)."

d. In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs 9–102*b* and *c*, above, as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.

e. **If the statement in paragraph 9–102 *c* , above applies, the supervisor must ensure that all relevant information is reported to the local command security official responsible for processing the investigative paperwork.**

f. **If the information seems to warrant adverse action, the command security official will immediately refer it to the Commander, CCF (PCCF–M), using DA Form 5248–R. CCF will process the cases in accordance with established procedures.**

g. **If the local command security official determines that the information is minor and does not warrant an adverse action, the PSI request should be forwarded to DIS. A summary of the derogatory information will be part of the investigative request packet. DIS will initiate the investigation and expand as appropriate. DIS will forward results of the investigation to CCF for adjudication.**

h. **It is important that immediate supervisors take an objective approach to the requirements in *b* and *c*, above, to ensure equity to both the subject of the investigation and national security.**

9–103. Individual responsibility

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

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

(1) Any form of contact, intentional or otherwise, with a citizen of a designated country, (app H) unless occurring as a function of one's official duties.

(2) Attempts by representatives or citizens of designated countries to cultivate friendships or to place one under obligation.

(3) Attempts by representatives or citizens of foreign countries to:

(a) Cultivate a friendship to the extent of placing one under obligation that they would not normally be able to reciprocate, or by offering money payments or bribery to obtain information of actual or potential intelligence value.

(b) Obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact.

(c) Coerce by blackmail, by threats against or promises of assistance to relatives living under foreign control, especially those living in a designated country.

(4) All personal foreign travel in advance.

(5) Any information of the type referred to in paragraph 2–200 or appendix I.

9–104. Coworker responsibility

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

Section II
Security Education

9–200. General

The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DOD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DOD personnel security program. Accordingly, heads of DOD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

9–201. Initial briefing

a. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this regulation shall be given an initial security briefing. **A record of this briefing will be maintained in the security office.** The briefing shall be in accordance with the requirements of paragraph 10–102, DOD 5200.1–R **(AR 380–5)** (reference (q)) and consist of the following elements:

(1) The specific security requirements of their particular job.

(2) The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts **(AR 381–12) (reference (rr)).**

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

(4) The penalties that may be imposed for security violations.

b. If an individual declines to execute Standard Form 189, "Classified Information Nondisclosure Agreement," the DOD Component shall initiate action to deny or revoke the security clearance of such person in accordance with paragraph 8–201 above.

9–202. Refresher briefing

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10–101, DOD 5200.1–R **(AR 380–5)** (reference (q)) shall be tailored to fit the needs of experienced personnel.

9–203. Foreign travel briefing

a. DOD Components will establish appropriate internal procedures requiring all personnel possessing a DOD security clearance to report to their security office all personal foreign travel in advance of the travel being performed. When travel patterns, or the failure to report such travel, indicate the need for investigation, the matter will be referred to the appropriate counterintelligence investigative agency.

b. Personnel having access to classified information shall be given a Foreign Travel Briefing by a counterintelligence agent, security specialist, security manager, or other qualified individual, as a defensive measure prior to travel to a designated country (app H) in order to alert them to their possible exploitation by hostile intelligence services. These personnel will also be debriefed upon their return. The briefings will be administered under the following conditions:

(1) Travel to or through designated country for any purpose.

(2) Attendance at international, scientific, technical, engineering, or other professional meetings in the United States or in any country outside the United States when it can be anticipated that representative(s) of designated countries will participate or be in attendance.

c. Individuals who travel frequently, or attend or host meetings of foreign visitors as described in *b*2, above, need not be briefed for each occasion, but shall be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

d. Records on such employees **of all personal foreign travel** will be maintained for 5 years **and may be in manual or automated form. Foreign travel records will be forwarded to the gaining command upon transfer of the individual. The losing command will retain a copy of the foreign travel record on file for 1 year after the individual's departure. Record of individuals who retire, separate, or terminate employment will be retained at the losing command until the expiration of the 5–year period. Data to be recorded are listed below:**

(1) **Name.**

(2) **SSN.**

(3) **Organization.**

(4) **Date security office was notified of proposed travel.**

(5) **Country or countries to be visited and inclusive dates.**

(6) **Date of foreign travel briefing (if travel meets criteria in *b* above) and name of person conducting briefing.**

(7) **Date of foreign travel debriefing (in accordance with *b* above) and name of person conducting debriefing.**

(8) **Purpose of visit.**

9–204. Termination briefing

a. Upon termination of employment, administrative withdrawal of security clearance, **revocation of security clearance,** or contemplated absence from duty or employment for 60 days or more, DOD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. **DA Form 2962 (Security Termination Statement and Debriefing Certificate) will be used for this purpose. Paragraph 10–104, AR 380–5 (reference (q)) applies.** This statement shall include:

(1) An acknowledgement that the individual has read the appropriate provisions of the Espionage Act and other criminal statutes and DOD regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;

(2) A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

(3) An acknowledgement that the individual will not communicate or transit classified information to any unauthorized person or agency; and

(4) An acknowledgement that the individual will report without delay to the FBI or the DOD Component concerned any attempt by any unauthorized person to solicit classified information.

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

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

d. In addition to the provisions of subparagraphs *a*, *b*, and *c*, above, DOD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers, and GS–16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy. **Senior civilian employees, GS–16 and above, will execute the DA Form 2962 at the employing activity at time of separation. The General Officer Management Office, ODCSPER, is the control office authorized to execute a DA Form 2962 for each separating general officer.**

Chapter 10
Safeguarding Personnel Security Investigative Records

10–100. General

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

10–101. Responsibilities

DOD authorities responsible for administering the DOD personnel security program and all DOD personnel authorized access to personnel security reports and records shall ensure that the use of such information is limited to that authorized by this regulation and that such reports and records are safeguarded as prescribed herein. The heads of DOD Components and the Deputy Under Secretary of Defense for Policy for the Office of the Secretary of Defense shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records as required by paragraphs 10–102 and 10–103 below.

10–102. Access restrictions

Access to personnel security investigative reports and personnel security clearance determination information shall be authorized

only in accordance with DOD Directives 5400.7 **(AR 340–17)** and 5400.11 **(AR 340–21)** (references (aa) and (bb)) and with the following:

a. DOD personnel security investigative reports shall be released outside of the DOD only with the specific approval of the investigative agency having authority over the control and disposition of the reports.

b. Within 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 paragraph 10–100. **Under no circumstances will foreign national employees of the Department of the Army be permitted access to investigative files concerning U.S. military, U.S. civilian, or foreign national employees, unless such employees shall themselves have been the subject of a favorable counterintelligence scoped background investigation.**

c. Access by subjects of personnel security investigative reports shall be afforded in accordance with DOD Directive 5400.11 **(AR 340–21)**(reference (bb)).

d. Access to personnel security clearance determination information shall be made available, other than provided for in *c* above, through security channels, only to DOD or other officials of the Federal Government who have an official need for such information.

10–103. Safeguarding procedures

Personnel security investigative reports and personnel security determination information **(to include NACI)** shall be safeguarded as follows:

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

b. 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.

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

d. 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 INVESTIGATION."

e. An individual's status with respect to a personnel security clearance or a Special Access authorization is to be protected as provided for in paragraph VI.C.6., DOD Directive 5400.7 **(AR 340–17)** (reference (aa)).

10–104. Records disposition

a. Personnel security investigative reports, to include OPM NACIs may be retained by DOD recipient organizations, **if the head of the Component deems it necessary to fulfill the requirements of paragraph 9–100 of this regulation**, only for the period necessary to complete the purpose for which they were originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization. All copies of such reports shall be destroyed within 90 days after completion of the required personnel security determination. Destruction shall be accomplished in the same manner as for classified information in accordance with paragraph 9–101, DOD 5200.1–R **(AR 380–5)** (reference (q)).

b. 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 action. That is, after the completion date of the investigation or the date on which the record was last released to an authorized user—whichever is later. Personnel security investigative reports resulting in an unfavorable administrative personnel action or court–martial or other investigations of a significant nature due to information contained in the investigation shall be destroyed 25 years after the date of the last action. Files in this latter category that are determined to be of possible historical value and those of widespread public or congressional interest may be offered to the National Archives after 15 years. **AR 381–45 (reference (tt)) applies.**

c. Personnel security investigative reports on persons who are considered for affiliation with DOD will be destroyed after 1 year if the affiliation is not completed.

10–105. Foreign source information

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

Chapter 11
Program Management

11–100. General

To ensure uniform implementation of the DOD personnel security program throughout the Department, program responsibility shall be centralized at theDOD Component level.

11–101. Responsibilities

a. The Deputy Under Secretary of Defense for Policy shall have primary responsibility for providing guidance, oversight, development and approval for policy and procedures governing personnel security program matters within the Department:

(1) Provide program management through issuance of policy and operating guidance.

(2) Provide staff assistance to the DOD Components and Defense Agencies in resolving day–to–day security policy and operating problems.

(3) Conduct inspections of the DOD Components for implementation and compliance with DOD security policy and operating procedures.

(4) Provide policy, oversight, and guidance to the Component adjudication functions.

(5) Approve, coordinate and oversee all DOD personnel security research initiatives and activities.

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

c. The heads of the Components shall ensure that:

(1) The DOD personnel security program is administered within their area of responsibility in a manner consistent with this regulation.

(2) A single authority within the office of the head of the DOD Component is assigned responsibility for administering the program within the Component.

(3) Information and recommendations are provided the Deputy Under Secretary of Defense for Policy and the General Counsel at their request concerning any aspect of the program.

d. **The Deputy Assistant Secretary of the Army for Civilian Personnel, Nonappropriated Funds, and Security Policy will ensure the implementation of DOD Directive 5200.2 and DOD 5200.2–R. The DASA (SAMR–PSP) will conduct oversight to include approving and disapproving of security–related policy and will provide guidance, as needed, on Army personnel security policy in its broadest dimensions.**

e. **The DCSINT is responsible for formulating policy governing —**

(1) **Army personnel security.**

(2) **Submitting PSI requests.**

(3) **Adjudicating personnel security.**

(4) **Continually assessing the suitability of individuals for access to classified information.**

f. **The Deputy Chief of Staff for Personnel (DCSPER) is responsible for—**

(1) **Accessing personnel for the total force.**

(2) **Determining personnel classification and standards.**

(3) **Adjudicating centralized personnel security.**

(4) **Formulating personnel management policy and procedures in compliance with existing security standards and criteria.**

(5) **Developing automation architecture for integrating the Total Army Information Systems.**

(6) **Using designation criteria to determine the number of civilian positions designated as sensitive. Records of sensitive and nonsensitive positions will be maintained by the servicing civilian personnel office. Those individuals authorized to designate sensitive positions will inform the servicing civilian personnel office of any change in position sensitivity.**

g. **The Commander, CCF, is responsible for the centralized adjudication, granting, revocation, and denial of personnel security clearances and SCI access eligibility determinations. The Commander, CCF, is authorized to suspend or direct the suspension of access to classified information.**

h. **Commanders, Army Staff heads, and supervisors are responsible for implementing the personnel security provisions of this regulation. Personnel security functions are normally delegated to the installation DSEC/security manager/G2, who will—**

(1) **Initiate requests for PSIs.**

(2) **Suspend an individual's access to classified information.**

(3) **Request security clearances.**

(4) **Grant interim security clearances.**

(5) **Report any adverse information.**

(6) **Assist personnel in completing applicable investigative forms.**

(7) **Conduct oversight visits of subordinate units at least once every 2 years.**

11–102. Reporting requirements

a. Personnel security program management data will be developed and submitted by **1 November** each year for the preceding fiscal year in a report to the Deputy Under Secretary of Defense for Policy **DCSINT, ATTN: DAMI–CIS, Washington, DC 20310–1051.** The information required below is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and Congress. The report will cover the preceding fiscal year, broken out by clearance category, according to officer, enlisted, civilian or contractor status.

b. **The Commander, CCF, will report the following:**

(1) Number of TOP SECRET, SECRET, and CONFIDENTIAL clearances issued;

(2) Number of TOP SECRET, SECRET, and CONFIDENTIAL clearances denied;

(3) Number of TOP SECRET, SECRET, and CONFIDENTIAL clearances revoked;

(4) Number of SCI access determinations issued;

(5) Number of SCI access determinations denied;

(6) Number of SCI access determinations revoked;

(7) Number of actions which resulted in nonappointment or nonselection to a sensitive position;

(8) Number of personnel adjudicating personnel security cases on a full– or part– time basis;

(9) Number of man–years expended in adjudicating personnel security cases.

c. **MACOM commanders and heads of Army Staff agencies will consolidate reports submitted by their subordinate units and field operating agencies pertaining to the following data:**

(1) Total number of personnel holding a clearance for TOP SECRET, SECRET, CONFIDENTIAL, and sensitive compartmented information as of the end of the fiscal year.

(2) Total number of personnel authorized access to TOP SECRET, SECRET, CONFIDENTIAL, and sensitive compartmented information as of the end of the fiscal year.

(3) Number of TOP SECRET billets established (para 3–104).

(4) Number of civilian positions designated sensitive, by designation criteria.

(5) The number of limited access authorizations in effect (in accordance with para 3–403).

d. This reporting requirement has been assigned report control symbol DD–POL(A)1749.

11–103. Inspections

The heads of DOD Components shall ensure that personnel security program matters are included in their administrative inspection programs.

Appendix A
References

This appendix has been moved to paragraph 1–100.

Appendix B
Investigative Scope

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

B–1. National Agency Check (NAC)

At a minimum, the first three of the described agencies (DCII, FBI/HQ, and FBI/ID) below shall be included in each complete NAC; however, a NAC may also include a check of any or all of the other described agencies, if appropriate.

a. DCII records consist of an alphabetical index of personal names and impersonal titles that appear as subjects or incidentals in investigative documents held by the criminal, counterintelligence, fraud, and personnel security investigative activities of the three military departments, DIS, Defense Criminal Investigative Service (DCIS), and the National Security Agency. DCCI records will be checked on all subjects of DOD investigations.

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

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

d. OPM. The files of OPM contain the results of investigations conducted by OPM under Executive Orders 9835 and 10450 (references (ff) and (g)), those requested by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE) and those requested since August 1952 to serve as a basis for "Q" clearances. Prior to that date, "Q" clearance investigations were conducted by the FBI. A "Q" clearance is granted to individuals who require access to DOE information. In order to receive a "Q" clearance, a full field background investigation must be completed on the individual requiring access in accordance with the Atomic Energy Act of 1954 (reference (gg)). Also on file are the results of investigations on the operation of the Merit System, violations of the Veterans Preference Act, appeals of various types, fraud and collusion in Civil Service examinations and related matters, data on all Federal employment, and an index of all BIs on civilian employees or applicants completed by agencies of the executive branch of the U.S Government. The OPM files may also contain information relative to U.S. citizens who are, or who were, employed by a United Nations organization or other public international organization such as the Organization of American States. OPM records are checked on all persons who are, or who have been, civilian employees of the U.S. Government; or U.S. citizens who are, or who have been, employed by a United Nations organization or other public international organization; and on those who have been granted security clearances by the NRC or DOE.

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

(1) An alien in the United States, or

(2) A naturalized citizen whose naturalization has not been verified, or

(3) An immigrant alien, or

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

f. State Department. The State Department maintains the following records:

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

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

g. Central Intelligence Agency (CIA). The files of CIA contain information on present and former employees, including members of the Office of Strategic Services (OSS), applicants for employment, foreign nationals, including immigrant aliens in the United States, and U.S. citizens traveling outside the United States after July 1, 1946. These files shall be checked under the following guidelines.

Table B–1
Criteria for CIA Checks

Investigation: NAC, DNACI, or ENTNAC **Criteria for CIA checks:** Residence anywhere outside of the United States for a year or more since age 18 except under the auspices of the United States Government; and travel, education, residence, or employment since age 18 in any designated country (app H).
Investigation: BI **Criteria for CIA checks:** Same as NAC, DNACI, and ENTNAC requirements plus travel, residence, employment, and education outside the United States for more than a continuous 3–month period during the past 5 years, or since age 18, except when under the auspices of the Government.
Investigation: SBI **Criteria for CIA checks:** Same as BI requirements except the period of the investigation will cover the past 15 years, or since age 18. Also when subject's employment, education, or residence has occurred overseas for a period of more than 1 year under the auspices of the U.S. Government, such checks will be made.

These files shall also be checked if subject has been an employee of CIA or when other sources indicate that CIA may have pertinent information.

h. Military Personnel Record Center files are maintained by separate departments of the Armed Forces, General Services Administration and the Reserve Records Centers. They consist of the Master Personnel Records of retired, separated, reserve, and active duty members of the Armed Force. These records shall be checked when the requester provides required identifying data indicating service during the last 15 years.

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

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

B–2. DOD National Agency Check and written inquiries (DNACI):

a. Scope. The time period covered by the DNACI is limited to the most recent 5 years, or since the 18th birthday, whichever is shorter, provided that the investigation covers at least the last 2 full

years of the subject's life, although it may be extended to the period necessary to resolve any questionable or derogatory information. No investigation will be conducted prior to an individual's 16th birthday. All DNACI investigation information will be entered on the DD Form 398–2 and FD–Form 258 and forwarded to the Defense Investigative service **C–4**, app C).

b. Components of a DNACI:

(1) *NAC.* This is the same as described in paragraph **B–**1, above.

(2) *Credit.*

(a) A credit bureau check will be conducted to cover the 50 States, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, at all locations where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months (cumulative) during the past 5 years.

(b) When information developed reflects unfavorably upon a person's current credit reputation or financial responsibility, the investigation will be expanded as necessary.

(3) *Employment.*

(a) Non–Federal employment

1. Verify, via written inquiry, all employment within the period of investigation with a duration of 6 months or more. Current employment will be checked regardless of duration.

2. If all previous employments have been less than 6 months long, the most recent employment, in addition to the current, will be checked in all cases.

3. Seasonal holiday, part–time and temporary employment need not be checked unless subparagraph 2, above, applies.

(b) Federal employment. All Federal employment (to include military assignments) within the period of investigation will be verified by the requester through locally available records, and a statement reflecting that such checks have been favorably accomplished will be contained in the investigative request. Those that cannot be verified in this fashion will be accomplished via written inquiry by DIS (within the 50 United States, Puerto Rico, Guam, and the Virgin Islands).

B–3. Background investigation (BI)

The period of investigation for the BI is 5 years and applies to military, civilian, and contractor personnel.

a. NAC. See paragraph **B–**1, above.

b. Local agency checks (LACs). Same as paragraph **B–**4*j*, below, except period of coverage is 5 years.

c. Credit checks. Same as paragraph **B–**4*i*, below.

d. Subject interview (SI). This is the principal component of a BI. In some instances an issue will arise after the primary SI and a secondary interview will be conducted. Interviews in the latter category are normally "issue" interviews that will be reported in the standard BI narrative format.

e. Employment records. Employment records will be checked at all places where employment references are interviewed with the exception of current Federal employment when the requester indicates that such employment has been verified with favorable results.

f. Employment reference coverage. A minimum of *three references, either supervisors or coworkers,* who have knowledge of the SUBJECT's activities in the work environment will be interviewed. At least one employment reference at the current place of employment will always be interviewed with the exception of an individual attending military basic training, or other military training schools lasting less than 90 days. However, if the SUBJECT has only been at the current employment for less than 6 months, it will be necessary to go not only to his or her current employment (for example, for one employment reference) but also to the preceding employment of at least 6 months for additional employment references. If the SUBJECT has not had prior employment of at least 6 months, interview(s) will be conducted at the most recent short–term employment in addition to the current employment.

g. Developed and listed character references. A minimum of three developed character references (DCRs) whose combined association with the subject covers the entire period of investigation will be interviewed. If coverage cannot be obtained through the DCRs, a listed character reference (LCR) will be contacted to obtain coverage.

h. Unfavorable information. Unfavorable information developed in the field will be expanded.

B–4. Special background investigation (SBI)

a. Components of an SBI. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is the shorter period, provided that the investigation covers at least the last 2 full years of the subject's life. No investigation will be conducted for the period prior to an individual's 16th birthday. Emphasis shall be placed on peer coverage whenever interviews are held with personal sources in making education, employment, and reference (including developed) contacts.

b. NAC. In addition to conducting a NAC on the subject of the investigation, the following additional requirements apply:

(1) A DCII, FBI/ID name check only and FBI/HQ check shall be conducted on subject's current spouse or cohabitant. In addition, such other national agency checks as deemed appropriate based on information on the subject's SPH or PSQ shall be conducted.

(2) A check of FBI/HQ files on members of subject's immediate family who are aliens in the United States or immigrant aliens who are 18 years of age or older shall be conducted. As used throughout the regulation, members of subject's immediate family include the following:

(a) Current spouse.

(b) Adult children, 18 years of age or older, by birth, adoption, or marriage.

(c) Natural, adopted, foster, or stepparents.

(d) Guardians.

(e) Brothers and sisters either by birth, adoption, or remarriage of either parent.

(3) The files of CIA shall be reviewed on alien members of subject's immediate family who are 18 years of age or older, regardless of whether or not these persons reside in the United States.

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

(a) Aliens in the United States, or

(b) Naturalized U.S. citizens whose naturalization has not been verified in a prior investigation, or

(c) Immigrant aliens, or

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

c. Birth. Verify subject's date and place of birth (DPOB) through education, employment and/or other records. Verify through Bureau of Vital Statistics (BVS) records if not otherwise verified under subparagraph *d,* below, or if a variance is developed.

d. Citizenship. Subject's citizenship status must be verified in all cases. U.S. citizens who are subjects of investigation will be required to produce documentation that will confirm their citizenship. Normally, such documentation should be presented to the DOD Component concerned prior to the initiation of the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that the designated authority in the DOD Component will be provided with the documentation prior to the issuance of a clearance. DIS will not check the BVS for native–born U.S. citizens except as indicated in subparagraph c, above. In the case of foreign–born U.S. citizens, DIS will check I&NS records. The citizenship status of all foreign–born members of subject's immediate family shall be verified. Additionally, when the investigation indicates that a member of subject's immediate family has not obtained U.S. citizenship after having been eligible for a considerable period of time, an attempt should be made to determine the reason. The documents listed below are acceptable for proof of U.S. citizenship for personnel security determination purposes:

(1) A birth certificate must be presented if the individual was born in the United States. To be acceptable, the certificate must show that the birth record was filed shortly after birth and must be

certified with the registrar's signature and the raised, impressed, or multicolored seal of his or her office except for States or jurisdictions which, as a matter of policy, do not issue certificates with a raised or impressed seal. Uncertified copies of birth certificates are not acceptable.

(a) A delayed birth certificate (a record filed more than 1 year after the date of birth) is acceptable provided that it shows that the report of birth was supported by acceptable secondary evidence of birth as described in subparagraph (b) below.

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

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

(2) A certificate of naturalization shall be submitted if the individual claims citizenship by naturalization.

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

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

(5) A passport or one in which the individual was included will be accepted as proof of citizenship.

e. Education.

(1) Verify graduation or attendance at institutions of higher learning in the United States within the last 15 years, if such attendance was not verified during a prior investigation.

(2) Attempts will be made to review records at overseas educational institutions when the subject resided overseas in excess of 1 year.

(3) Verify attendance or graduation at the last secondary school attended within the past 10 years if there was no attendance at an institution of higher learning within the period of investigation.

(4) Verification of attendance at military academies is only required when the subject failed to graduate.

f. Employment.

(1) *Non–Federal employment.* Verify all employment within the period of investigation to include seasonal, holiday, Christmas, part–time, and temporary employment. Interview one supervisor and one coworker at subject's current place of employment as well as at each prior place of employment during the past 10 years of 6 months or longer. The interview requirement for supervisors and coworkers does not apply to seasonal, holiday, Christmas, part–time, and temporary employment (4 months or less) unless there are unfavorable issues to resolve or the letter of inquiry provides insufficient information.

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

(3) *Military employment.* Military service for the last 15 years shall be verified. The subject's duty station, for the purpose of interview coverage, is considered as a place of employment. One supervisor and one coworker shall be interviewed at subject's current duty station if subject has been stationed there for 6 months or more; additionally, a supervisor and a coworker at subject's prior duty stations where assigned for 6 months or more during the past 10 years shall be interviewed.

(4) *Unemployment.* Subject's activities during all periods of unemployment in excess of 30 consecutive days, within the period of investigation, that are not otherwise accounted for shall be verified.

(5) When an individual has resided outside the United States continuously for over 1 year, attempts will be made to confirm overseas employments as well as conduct required interviews of a supervisor and coworker.

g. References. Three developed character references who have sufficient knowledge of subject to comment on his or her background, suitability, and loyalty shall be interviewed personally. Efforts shall be made to interview developed references whose combined association with subject covers the full period of the investigation with particular emphasis on the last 5 years. Employment, education, and neighborhood references, in addition to the required ones, may be used as developed references provided that they have personal knowledge concerning the individual's character, discretion, and loyalty. Listed character references will be interviewed only when developed references are not available or when it is necessary to identify and locate additional developed character references or when it is necessary to verify subject's activities (e.g., unemployment).

h. Neighborhood investigation. Conduct a neighborhood investigation to verify each of subject's residences in the United States of a period of 6 months or more on a cumulative basis, during the past 5 years or during the period of investigation, whichever is shorter. During each neighborhood investigation, interview two neighbors who can verify subject's period of residence in that area and who were sufficiently acquainted to comment on subject's suitability for a position of trust. Neighborhood investigations will be expanded beyond this 5–year period only when there is unfavorable information to resolve in the investigation.

i. Credit. Conduct credit bureau check in the 50 States, the District of Columbia, Puerto Rico, and overseas (where APO/FPO addresses are provided) at all places where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months or more, on a cumulative basis, during the last 7 years or during the period of the investigation, whichever is shorter. When coverage by a credit bureau is not available, credit references located in that area will be interviewed. Financial responsibility, including unexplained affluence, will be stressed in all reference interviews.

j. Local agency checks (LACs). LACs, including State central criminal history record repositories, will be conducted on subject at all places of residence to include duty stations and/or home ports, in the 50 States, the District of Columbia, and Puerto Rico, where residence occurred during the past 15 years or during the period of investigation, whichever is shorter. If subject's place of employment and/or education is serviced by a different law enforcement agency than that servicing the area of residence, LACs shall be conducted also in these areas.

k. Foreign travel. If subject has been employed or educated or has traveled or resided outside of the United States for more than 90 days during the period of investigation, except under the auspices of the U.S. Government, additional record checks during the NAC shall be made in accordance with paragraph **B–**1*f* of this appendix. In addition, the following requirements apply:

(1) *Foreign travel not under the auspices of the U.S. Government.* When employment, education, or residence has occurred overseas for more than 90 days during the past 15 years or since age 18, which was not under the auspices of the U.S. Government, a check of records will be made at the Passport Office of the Department of State, the CIA, and other appropriate agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas to cover significant employment, education, or

residence and to determine whether any lasting foreign contacts or connections were established during this period. If the individual has worked or lived outside of the United States continuously for over 1 year, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

(2) *Foreign travel under the auspices of the U.S. Government.* When employment, education, or residence has occurred overseas for a period of more than 1 year, under the auspices of the U.S. Government, a record check will be made at the Passport Office of the Department of State, the CIA, and other appropriate agencies. Efforts shall be made to develop sources (generally in the United States) who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. Additionally, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available tothe United States Government in the foreign country in which the individual resided.

l. Foreign connections. All foreign connections (friends, relatives, and/or business connections) of subject and immediate family in the United States or abroad, except where such association was the direct result of subject's official duties with the U.S. Government, shall be ascertained. Investigation shall be directed toward determining the significance of foreign connections on the part of subject and the immediate family, particularly where the association is or has been with persons whose origin was within a country whose national interests are inimical to those of the United States. When subject or his or her spouse has close relatives residing in a Communist–controlled country, or subject has resided, visited, or traveled in such a country, not under U.S. Government auspices, the provisions of paragraph 2–308*c* of this regulation apply.

m. Organizations. Efforts will be made during reference interviews and record reviews to determine if subject and/or the immediate family has, or formerly had, membership in, affiliation with, sympathetic association towards, or participated in any foreign or domestic organization, association, movement, group, or combination of persons of the type described in paragraphs 2–200*a* through *d* of this regulation.

n. Divorce. Divorces, annulments, and legal separations of subject shall be verified only when there is reason to believe that the grounds for the action could reflect on subject's suitability for a position of trust.

o. Military service. All military service and types of discharge during the last 15 years shall be verified.

p. Medical records. Medical records shall not be reviewed unless:

(1) The requester indicates that subject's medical records were unavailable for review prior to submitting the request for investigation, or

(2) The requester indicates that unfavorable information is contained in subject's medical records, or

(3) The subject lists one or more of the following on the Statement of Personal History or Personnel Security Questionnaire:

(a) A history of mental or nervous disorders.

(b) That subject is now or has been addicted to the use of habit–forming drugs such as narcotics or barbiturates or is now or has been a chronic user to excess of alcoholic beverages.

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

B–5. Periodic reinvestigation (PR)

a. Each DOD military, civilian, consultant, and contractor employee (to include foreign nationals holding a limited access authorization) occupying a critical–sensitive position, possessing a TOP SECRET clearance, or occupying a special access program position **or whose MOS requires access to TOP SECRET and/or SCI**, shall be the subject of a PR initiated **not later than** 5 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years.

(1) **If there has been a break in the individual's military service, DA civilian employment, or contractor employment (for contractor employees who require access to SCI) of more than 12 months, a PR is not acceptable. A BI or SBI, as appropriate, is required.**

(2) **If the previous investigation (BI, SBI, or PR) is more than 6 years old, a PR is not acceptable. A BI or SBI, as appropriate, is required to cover the period since the last investigation.**

b. Minimum investigative requirements. A PR shall include the following minimum scope.

(1) *NAC.* A valid NAC on the subject will be conducted in all cases. Additionally, for positions requiring SCI access, checks of DCII, FBI/HQ, FBI/ID name check only, and other agencies deemed appropriate will be conducted on the subject's current spouse or cohabitant, if not previously conducted. Additionally, NACs will be conducted on immediate family members, 18 years of age or older, who are aliens and/or immigrant aliens, if not previously accomplished.

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

(3) *Subject interview.* The interview should cover the entire period of time since the last investigation, not just the last 5–year period. Significant information disclosed during the interview, which has been satisfactorily covered during a previous investigation, need not be explored again unless additional relevant information warrants further coverage. An SI is not required if one of the following conditions exist:

(a) The subject is aboard a deployed ship or in some remote area that would cause the interview to be excessively delayed.

(b) The subject is in an overseas location serviced by the State Department or the FBI.

(4) *Employment.* Current employment will be verified. Military and Federal service records will not routinely be checked, if previously checked by the requester when PR was originally submitted. Also, employment records will be checked wherever employment interviews are conducted. Records need be checked only when they are locally available, unless unfavorable information has been detected.

(5) *Employment references.* Two supervisors or coworkers at the most recent place of employment or duty station of 6 months **will be interviewed**; if the current employment is less than 6 months, employment reference interviews will be conducted at the next prior place of employment **of** at least a 6–month duration.

(6) *Developed character references (DCRs).* Two developed character references who are knowledgeable of the subject will be interviewed. Developed character references who were previously interviewed will only be reinterviewed when other developed references are not available.

(7) *Local agency checks (LACs).* DIS will conduct local agency checks on the subject at all places of residence, employment, and education during the period of investigation, regardless of duration, including overseas locations.

(8) *Select scoping.* When the facts of the case warrant, additional

select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

Appendix C
Request Procedures

C–1. General

To conserve investigative resources and to ensure 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 this connection, it is particularly important that the provision of Executive Order 12356 (reference (j)) requiring strict limitations on the dissemination of official information and material be closely adhered to and that investigations requested for issuing clearances are limited to those instances in which an individual has a clear need for access to classified information. Similarly, investigations required to determine eligibility for appointment or retention in DOD, in either a civilian or military capacity, must not be requested in frequency or scope exceeding that provided for in this regulation. In view of the foregoing, the following guidelines have been developed to simplify and facilitate the investigative request process:

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

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

c. Ensure that request forms and prescribed documentation are properly executed in accordance with instructions;

d. Dispatch the request directly to the DIS Personnel Investigations Center;

e. Promptly notify the DIS Personnel Investigations Center **through CCF (PCCF–M)** if the investigation is no longer needed (notify OPM if a NACI is no longer needed; and

f. Limit access through strict need to know, thereby requiring fewer investigations.

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

C–2. National Agency Check (NAC)

When a NAC is requested, an original only of the DD Form 398–2 (National Agency Check Request) and a completed FD 258 (Applicant Fingerprint Card) are required. If the request is for an ENTNAC, an original only of the DD Form 398–2 and a completed DD Form 2280 (Armed Forces Fingerprint Card) are required. Those forms should be sent directly to: Personnel Investigation Center, Defense Investigative Service, P.O. Box 1083, Baltimore, MD 21203.

C–3. National Agency Check and written inquiries (NACI)

When a NACI is requested, an original and one copy of the SF **86 (Questionnaire for Sensitive Positions),** an SF 171 (Personal Qualifications Statement), and an SF 87 (U.S. Civil Service Commission Fingerprint Chart) shall be sent directly to: Office of Personnel Management,Bureau of Personnel Investigations, NACI Center, Boyers, PA 16018. The notation "ALL REFERENCES" shall be stamped immediately above the title at the top of the Standard Form 85.

C–4. DOD National Agency Check and written inquiries (DNACI)

a. When a DNACI is requested, one copy of DD Form 1879, an original and two copies of the DD Form 398–2 (National Agency Check Request), two copies of FD 258 (Fingerprint Card), and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to: Personnel Investigations Center, Defense Investigative Service, P.O. Box 1083, Baltimore, MD 21203.

b. The DD Form 398–2 must be completed to cover the most recent 5–year period. All information, to include items relative to residences and employment, must be complete and accurate to avoid delays in processing.

C–5. Special background investigation (SBI)/background investigation (BI)

a. When requesting a BI or SBI, one copy of DD Form 1879 (Request for Personnel Security Investigation), an original and four copies of DD Form 398 (Statement of Personnel History), two copies of FD 258, and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to: Personnel Investigations Center, Defense Investigative Service, P.O. Box 454, Baltimore, MD 21203.

b. For the BI and SBI, the DD Form 398 must be completed to cover the most recent 5– and 15–year period, respectively, or since the 18th birthday, whichever is shorter.

c. **When requesting an SBI, DD Form 398–2 must be submitted for the spouse or cohabitant. A DD Form 398–2 must also be submitted for immediate family members over 18 years of age who are not U.S. citizens.**

C–6. Periodic reinvestigation (PR)

a. PRs shall be requested only in such cases as are authorized by paragraphs 3–700 through 3–711 of this regulation.

(1) For a PR requested in accordance with paragraphs 3–700 through 3–711, the DD Form 1879 must be accompanied by the following documents:

(a) Original and four copies of DD Form 398.

(b) Two copies of FD–258.

(c) Original copy of DD Form 2221.

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

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

c. **The DD Form 398 completed for a BI PR will cover the most recent 5–year period and for an SBI PR it will be completed to cover the period from the date of the most recent SBI or SBI PR to present date.**

d. The PR request shall be sent to the address in paragraph **C–**5*a*, above.

C–7. Additional investigation to resolve derogatory or adverse information

a. Requests for additional investigation required to resolve derogatory or adverse information shall be submitted by DD Form 1879 (Request for Personnel Security Investigation) to: Defense Investigative Service, P.O. Box 454, Baltimore, MD 21203. Such requests shall set forth the basis for the additional investigation and describe the specific matter to be substantiated or disproved.

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

results of a recently completed NAC, NACI, or other related investigative reports available should also accompany the request.

C–8. Obtaining results of prior investigations

Requesters requiring verification of a specified type of personnel security investigation, and/or requiring copies of prior investigations conducted by the DIS shall submit requests by letter or message to: Defense Investigative Service Investigative Files Division, P.O. Box 1211, Baltimore, MD 21203. Message address: DIS PIC BALTIMORE MD/ /D0640. The request will include subject's name, grade, social security number, date and place of birth, and DIS case control number if known.

C–9. Requesting postadjudication cases

a. Requests pertaining to issues arising after adjudication of an investigation (post–adjudication cases) shall be addressed to DIS on a DD Form 1879 accompanied by a DD Form 398, when appropriate.

b. All requests for initial investigations will be submitted to PIC regardless of their urgency. If, however, there is an urgent need for a postadjudication investigation, or the mailing of a request to PIC for initiation of a postadjudication case would prejudice timely pursuit of investigative action, the DD Form 1879 may be directed for initiation, in CONUS, to the nearest DIS field office, and in overseas locations, to the military investigative service element supporting the requester (app J). The field element (either DIS or the military investigative agency) will subsequently forward either the DD Form 1879 or completed investigation to PIC.

c. A fully executed DD Form 1879 and appropriate supporting documents may not be immediately available. Further, a case that is based on sensitive security issues may be compromised by a request that the subject submit a DD Form 398. A brief explanation should appear on the DD Form 1879 which does not include complete supporting documentation.

C–10. Requests involving contractor employees

To preclude duplicative investigative requests and double handling of contractor employee cases involving access to classified information, all requests for investigation of contractor personnel must be submitted, using authorized industrial security clearance forms, for processing through the Defense Industrial Security Clearance Office, except for programs in which specific approval has been obtained from the Deputy Under Secretary of Defense for Policy to utilize other procedures.

C–11. Responsibility for proper documentation of requests

The official signing the request for investigation shall be responsible for ensuring that all documentation is completed in accordance with these instructions.

C–12. Requests involving Red Cross and USO employees

a. **The Red Cross and USO will prepare the request for NAC on prospective employees. DD Form 398–2 and FD Form 258 will be forwarded to the Defense Industrial Security Clearance Office (DISCO) for processing.**

b. **DISCO will make a determination as to the acceptability of the prospective employee. If the determination is favorable, the Red Cross or USO will be notified. All unfavorable determinations will be forwarded to the Director for Industrial Security Clearance Review Office of the Defense General Counsel for action. The applicant, Red Cross or USO, and the host commander will be advised of the final determination.**

c. **If derogatory information is received on a Red Cross or USO employee, the host command or Red Cross or USO will forward the information for review to: Defense Industrial Security Clearance Office, ATTN: DISCO–A, P.O. Box 2499, Columbus, OH 43216–5006.**

d. **DISCO will initiate any investigation necessary to resolve derogatory information.**

e. **If a Red Cross or USO employee requires a security clearance, the host commander will forward the request together with a copy of the DISCO acceptability determination to the Commander, CCF, for action. All security clearances will be granted by the Commander, CCF, for Red Cross and/or USO employees on Army installations.**

Appendix D
Tables for Requesting Investigations

Table D–1
Guide for requesting background investigations (BIs)

A	B	C
If the individual is a	and duties require	then a BI is required before
U.S. national military member, civilian, consultant, or contractor employee	TOP SECRET clearance	granting final clearance
U.S. national civilian employee	assignment to a “critical–sensitive” position	assignment to the position
U.S. national military member, civilian, or contractor employee	occupying a “critical” position in the Nuclear Weapon Personnel Reliability Program (PRP) (reference (s))	occupying a “critical” DOD position
U.S. national military member or civilian employee	granting or denying clearances	performing clearance functions
U.S. national military member or civilian employee	membership on security screening, hearing, or review board	appointment to the board
immigrant alien	limited access to SECRET or CONFIDENTIAL information	issuing limited access authorization (see note)
non–U.S. national employee, excluding immigrant alien,	limited access to SECRET or CONFIDENTIAL information	issuing limited access authorization
non–U.S. national nominee for military education and orientation program (from a country listed at app H)	education and orientation of military personnel	performing duties
U.S. national military member or DOD civilian or contractor employee	assignment to a category two Presidential support position	assignment
U.S. national military member or DOD civilian or contractor employee assigned to NATO	access to NATO COSMIC information	access may be granted

Notes:
BI will cover a 10–year scope.

Table D–2
Guide for requesting special background investigations (SBIs)

A	B	C
If the individual is a	then a SBI is required and duties require	before
U.S. national military member or DOD civilian, consultant, or contractor employee	access to SCI	granting access
	assignment to a category one Presidential support position	assignment
	access to SIOP–ESI	granting access
	assignment to the National Security Agency	assignment
	access to other Special Access programs approved under paragraph 3–506	granting access
	assignment to personnel security, counterintelligence, or criminal investigative or direct investigative support duties	assignment

Table D–3
Guide for requesting periodic reinvestigations (PRs)

A	B	C
If the individual is a	and duties require	then a PR is required
U.S. national military member or DOD civilian, consultant, or contractor employee	access to SCI	5 years from date of last SBI/BI or SBI PR
	TOP SECRET clearance	5 years from date of last SBI/BI or PR
	access to NATO COSMIC	5 years from date of last SBI/BI or PR
	assignment to Presidential support activities	5 years from date of last SBI/BI or PR

Table D–3
Guide for requesting periodic reinvestigations (PRs)—Continued

A	B	C
U.S. national civilian employee	assignment to a "critical–sensitive" position	5 years from last SBI/BI or PR
non–U.S. national employee	current limited access authorization to SECRET or CONFIDENTIAL information	5 years from last SBI/BI or PR
U.S. national military member	assignment to duties defined in paragraph 3–703.1 or requiring TS or SCI eligibility in accordance with AR 611–101 (reference (zz)), AR 611–112 (reference (aaa)), or AR 611–201 (reference (bbb))	5 years from last SBI/BI or PR

Table D–4
Guide for requesting DOD National Agency Check with written inquiries (DNACI) or NACI

A	B	C
If the individual is a	and duties require	then a DNACI/NACI is required
U.S. national military member or contractor employee	SECRET clearance Interim SECRET clearance	before granting clearance (see note 1) automatically (see note 2)
U.S. national civilian employee or consultant	SECRET clearance Interim SECRET clearance Appointment to "noncritical–sensitive" position	before granting clearance automatically (see note 3) before appointment
U.S. national military member or DOD civilian or contractor employee	occupying a "controlled" position in the Nuclear Weapon PRR (reference(s))	before assignment
applicant for appointment as a commisioned officer	commission in the Armed Forces	before appointment (after appointment for health professionals, chaplains, and attorneys, under conditions authorized by para 3–303 of this Regulation)
Naval Academy Midshipman, Military Academy Cadet, or Air Force Academy Cadet	enrollment	to be initiated 90 days after entry
Reserve Officer Training Corps Cadet or Midshipman	entry to advanced course or college scholarship program	to be initiated 90 days after entry

Notes:

1. First–term enlistees shall require an ENTNAC.
2. Provided DD Form 398–2 is favorably reviewed, local records check favorably accomplished, and DNACI initiated.
3. Provided an authority designated in appendix F finds delay in such appointment would be harmful to national security; favorably review of DD Form 389–2; NACI initiated; and favorable local records check accomplished.

Table D–5
Guide for requesting National Agency Checks (NACs)

A	B	C
If the individual is a	and duties require	then a NAC is required
first–term enlistee	retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT 3 work days after entry (see note 1)
prior service member reentering military service after break in Federal employment exceeding 1 year	retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT 3 work days after reentry
nominee for military education and orientation program	education and orientation of military personnel	before performing duties (see note 2)
U.S. national military or DOD civilian or contractor employee	access to restricted areas, sensitive information, or equipment as defined in paragraph 3–601	before authorizing entry
nonappropriated fund instrumentality (NAFI) civilian employee (reference (u))	appointment as NAFI custodian accountability for nonappropriated funds	before appointment before completion of probationary period

Table D–5
Guide for requesting National Agency Checks (NACs)—Continued

A	B	C
	fiscal responsibility as determined by NAFI custodian other "positions of trust"	before completion of probationary period before appointment
Persons requiring access to chemical agents	access to or security of chemical agents	before assignment
U.S. national, civilian employee nominee for customs inspection duties	waiver under provisions of paragraph 3–603	before appointment (see note 3)
Red Cross/United Service Organizations personnel	assignment with the Armed Forces overseas	before assignment (see note 4 for foreign national personnel)
U.S. national	a DOD building pass	prior to issuance
Foreign national employed overseas	no access to classified information	prior to employment (see note 4)

Notes:

1. Request ENTNAC only.
2. Except when personnel whose country of origin is listed at appendix H, a BI will be required (see para 3–611).
3. A NAC not over 5 years old suffices unless there has been a break in employment over 12 months. Then a current NAC is required.
4. In such cases, the NAC shall consist of: (a) host government law enforcement and security agency record checks at the city, State (Province), and national level, and (b) DCII.

Appendix E
Reporting of Nonderogatory Cases

A background investigation (BI) and special background investigation (SBI) shall be considered as devoid of significant adverse information unless they contain information listed below:

E–1. Incidents, infractions, offenses, charges, citations, arrests, suspicion or allegations of illegal use or abuse of drugs or alcohol, theft or dishonesty, unreliability, irresponsibility, immaturity, instability or recklessness, the use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

E–2. All indications of moral turpitude, heterosexual promiscuity, aberrant, deviant, or bizarre sexual conduct or behavior, transvestism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, wife swapping, window peeping, and similar situations from whatever source. Unlisted full–time employment or education; full–time education or employment that cannot be verified by any reference or record source or that contains indications of falsified education or employment experience. Records or testimony of employment, education, or military service where the individual was involved in serious offenses or incidents that would reflect adversely on the honesty, reliability, trustworthiness, or stability of the individual.

E–3. Foreign travel, education, visits, correspondence, relatives, or contact with persons from or living in a designated country (app H).

E–4. Mental, nervous, emotional, psychological, psychiatric, or character disorders/behavior or treatment reported or alleged from any source.

E–5. Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy, or evidence of living beyond the individual's means.

E–6. Any other significant information relating to the criteria included in *a* through *q* of paragraph 2–200 or appendix I of this regulation.

Appendix F
Personnel Security Determination Authorities

F–1. Officials authorized to grant, deny or revoke personnel security clearances (TOP SECRET, SECRET, and CONFIDENTIAL):

a. Secretary of Defense and/or designee.
b. Secretary of the Army and/or designee.
c. Secretary of the Navy and/or designee.
d. Secretary of the Air Force and/or designee.
e. Chairman, Joint Chiefs of Staff, and/or designee.
f. Directors of the Defense Agencies and/or designee.
g. Commanders of the Unified and Specified Commands and/or designee.
h. **DCSINT and/or designee.**
i. Commander, CCF, and/or designee.

F–2. Officials authorized to grant limited access authorizations:

a. Secretaries of the Military Departments and/or designees.
b. Director, Washington Headquarters Services, for OSD and/or designee.
c. Chairman, JCS, and/or designee.
d. Directors of the Defense Agencies and/or designees.
e. Commanders, Unified and Specified Commands, and/or designees.
f. **Heads of HQDA Staff agencies.**
g. **Commanders of MACOMs.**
h. Commander, CCF.

F–3. Officials authorized to grant access to SCI:

a. Director, NSA—for NSA.
b. Director, DIA—for OSD, OJCS, and Defense Agencies.
c. Senior Officers of the Intelligence Community of the Army (DCSINT), Navy, and Air Force—for their respective Military Departments, or their single designee.
d. **Commander, CCF.**

F–4. Officials authorized to certify personnel under their jurisdiction for access to restricted data (to include critical nuclear weapon design information):

See enclosure to DOD Directive 5210.2 **(AR 380–150)** (reference (z)).

F–5. Officials authorized to approve personnel for assignment to Presidential support activities:

a. The Executive Secretary to the Secretary.
b. Deputy Secretary of Defense or designee.

F–6. Officials authorized to grant access to SIOP–ESI:

a. Director of Strategic Target Planning.
b. Director, Joint Staff, OJCS.
c. Chief of Staff, U.S. Army.
d. Chief of Naval Operations.
e. Chief of Staff, U.S. Air Force.
f. Commendant of the Marine Corps.
g. Commanders of Unified and Specified Commands.
h. The authority to grant access delegated above may be further delegated in writing by the above officials to the appropriate subordinates.

F–7. Officials authorized to designate sensitive positions:

a. Heads of DOD Components or their designees for critical–sensitive positions.
(1) **Under Secretary of the Army.**
(2) **Assistant secretaries of the Army.**
(3) **Deputy assistant secretaries of the Army.**
(4) **Chief of Staff.**
(5) **Heads of HQDA Staff agencies.**
(6) **Commanders of MACOMs. Note: These officials may redelegate this authority to subordinate commanders as deemed necessary.**
b. Organizational commanders for noncritical–sensitive positions.

F–8. Nonappropriated Fund positions of trust

Officials authorized to designate Nonappropriated Fund positions of trust: Heads of DOD Components and/or their designees.
a. **Under Secretary of the Army.**
b. **Assistant secretaries of the Army.**
c. **Deputy assistant secretaries of the Army.**
d. **Chief of Staff.**
e. **Heads of HQDA Staff agencies.**
f. **Commanders of MACOMs.**
g. **Organizational commanders.**

Appendix G
Guidelines for Conducting Prenomination Personal Interviews

G–1. Purpose

The purpose of the personal interview is to assist in determining the acceptability of an individual for nomination and further processing for a position requiring an SBI.

G–2. Scope

Questions asked during the course of a personal interview must have a relevance to a security determination. Care must be taken not to inject improper matters into the personal interview. For example, religious beliefs and affiliations, beliefs and opinions regarding racial matters, political beliefs and affiliations of a nonsubversive nature, opinions regarding the constitutionality of legislative policies, and affiliations with labor unions and fraternal organizations

are not proper subjects for inquiry. Department of Defense representatives conducting personal interviews should always be prepared to explain the relevance of their inquiries. Adverse inferences shall not be drawn from the refusal of a person to answer questions the relevance of which has not been established.

G–3. The interviewer

Except as prescribed in paragraph **G–2** above, persons conducting personal interviews normally will have broad latitude in performing this essential and important function and, therefore, a high premium must necessarily be placed upon the exercise of good judgment and common sense. To ensure that personal interviews are conducted in a manner that does not violate lawful civil and private rights or discourage lawful political activity in any of its forms, or intimidate free expression, it is necessary that interviewers have a keen and well–developed awareness of and respect for the rights of interviewees. Interviewers shall never offer an opinion as to the relevance or significance of information provided by the interviewee to eligibility for access to SCI. If explanation in this regard is required, the interviewer will indicate that the sole function of the interview is to obtain information and that the determination of relevance or significance to the individual's eligibility will be made by other designated officials.

G–4. Interview procedures

a. The head of the DOD Component concerned shall establish uniform procedures for conducting the interview that are designed to elicit information relevant to making a determination of whether the interviewee, on the basis of the interview and other locally available information (DD 398, Personnel Security Investigation Questionnaire, personnel records, security file, etc.), is considered acceptable for nomination and further processing.

b. Such procedures shall be structured to ensure the interviewee his full rights under the Constitution of the United States, the Privacy Act of 1974 (reference (m)), and other applicable statutes and regulations.

G–5. Protection of interview results

All information developed during the course of the interview shall be maintained in personnel security channels and made available only to those authorities who have a need to know in connection with the processing of an individual's nomination for duties requiring access to SCI or those who need access to information either to conduct the required SBI or to adjudicate the matter of the interviewee's eligibility for access to SCI, or as otherwise authorized by Executive order or statute.

G–6. Acceptability determination

a. The determination of the interviewee's acceptability for nomination for duties requiring access to sensitive information shall be made by the commander, or designee, of the DOD organization that is considering nominating the interviewee for such duties.

b. Criteria guidelines contained in DCID 1/14 (reference (l)), upon which the acceptability for nomination determination is to be based, shall be provided to commanders of DOD organizations who may nominate individuals for access to SCI and shall be consistent with those established by the Senior Officer of the Intelligence Community of the Component concerned with respect to acceptability for nomination to duties requiring access to SCI.

G–7. Standard subject interview guidance

Guidance for conducting the interview is furnished below. The interviewee will be advised that the interview is a necessary part of an investigation which has been requested in connection with his or her nomination for access to SCI. The following outline illustrates the basic questions directed at the interviewee during a routine interview. It is impossible to provide a series of questions to cover every situation. However, the basis for all questions is the interviewee's DD Form 398 (Statement of Personal History), and the order of the questions should follow those of the DD Form 398 in most instances. Questions concerning items of the DD Form 398, which are not specifically addressed below, should center on completeness and accuracy of the information provided by the interviewee.

a. ***Items 1, 3, and 4 ("Name, Alias, and Address").*** **Explore the possible use of an alias, nickname, or other name other than subject's name as listed in Item 1. Any changes of name by court action or otherwise? If so, obtain details. Any use of a professional or stage name? Has subject always been known by the name listed in Item 1? Determine whether address is current or different from SPH.**

b. ***Item 5 (Date and Place of Birth, Place Certificate Recorded, Physical Appearance).*** **Ensure that there is no question as to subject's date and place of birth. Does subject have any scars, physical defects, or distinguishing marks? Determine origin of any scars if pertinent (for example, wrist scars—suicide attempt; other cars—fights).**

c. ***Item 6 (Nervous Disorders, Drugs, Alcohol).***

(1) ***Mental, nervous, or emotional problems.*** **Any consultations with psychiatrists, psychologists, or psychoanalysts? Any of the above by any member of subject's immediate family? If subject responds positively to the above, obtain details if the problem concerns the subject himself or herself. The following should be covered under this heading: timeframe of the illness, medication, extent of the treatment, complete identity of doctors or counselors, subject's symptoms, subject's explanation for the cause of the symptoms, subject's current mental and physical health. Also, note the following**

(a) **Any consultations with, treatment, or analysis by a psychiatrist (military or civilian doctors, if subject is military).**

(b) **Any physical disorders predicated on mental, emotional, or nervous problems.**

(c) **Any member of family having history of such disorders.**

(d) **Any attempt at suicide. (Explore discretely, if indicated by answers to other questions.)**

(2) ***Drugs.*** **Any experimentation, use, or addiction to any narcotics, barbiturates, marijuana, LSD, or any dangerous or illegal drugs? Any use on the part of immediate members of subject's family? Has subject ever been present while someone was using the above drugs? If yes, determine the circumstances. If there appears to be more than an experimental use on subject's part, then terminate the interview for handling by appropriate authorities. If only experimental, determine drugs used, circumstances, possibility of other use, effect on subject, reason for use, extent of subject's knowledge as to the legality of use, and future intent regarding use. Any involvement on subject's part with the police because of the above? Obtain address of anyone who can substantiate subject's story. Any illicit use on part of family and friends? (Followup questions regarding use by friends only if there are indications that subject is susceptible to undue influence, or that subject's reputation might suffer as a result of such association.)**

(3) ***Alcohol.*** **Have subject describe his or her alcohol drinking habits and any problems associated with alcohol consumption (for example, involvement with police, embarrassing situations, fights, or marital difficulties). Any alcohol problems in subject's immediate family? If subject appears to have a problem with the use of alcohol, obtain details on the rate of consumption, behavior patterns, as well as unfavorable information associated with his or her drinking.**

d. ***Item 8 (Military Service).*** **Ensure that all periods of active duty, to include discharge for reenlistment, are covered. If discharged other than honorably, obtain details. Also, note the following:**

(1) **Verify dates and type(s) of discharge.**

(2) **For enlisted personnel, enter in Item 8a the date of commencement of current tour. Each previous enlistment and/or tour of duty is listed consecutively in Item 8c, even though immediate reenlistment occurred after each tour.**

(3) **Punishment under Article 15, UCMJ.**

(4) **Subject is required to list all courts–martial in Item 8 regardless of length of time and changes in military law. If**

subject was acquitted by court martial, he or she still must list it.

(5) **Any unfavorable involvement with military law enforcement authority.**

(6) **Has interviewee ever been the subject of investigations by military criminal or counterintelligence agencies, except for routine security clearance investigations?**

(7) **Any difficulties with military or civilian supervisors. Any unfavorable action, such as written reprimands or unsatisfactory efficiency reports, that might be developed through review of permanent personnel records.**

e. ***Item 11 (Relatives and Alien Friends in Foreign Countries).*** **Does subject or spouse have any foreign relatives living in the United States or elsewhere? Be especially concerned if subject's or spouse's parents were born in a foreign country. Has subject ever heard that he or she has any foreign relatives? Has he or she ever written to any foreign relatives or met them? Does subject's spouse have any foreign friends? Be sure that subject understands what a friend is, and that he or she does not confuse this with an acquaintance or a coworker with whom there is no close friendship. Obtain identifying data to include full name, occupation, age, address, and citizenship of the person, extent of contact, and correspondence with the person. Obtain details particularly for any Communist–bloc national under this heading.**

f. ***Item 12 (Foreign Travel).*** **Ensure that subject lists all foreign travel, including Mexico and Canada. Obtain full details regarding any travel within bloc (Communist–controlled) countries; date, place, and method of entry and exit; contact with bloc nationals before, during, and after travel; black market or other illegal activities; problems with police, customs, or passport officials; illnesses while in country; purpose for visits; embarrassing, compromising, or questionable activities while in the country. Has subject had any unfavorable involvement with police officers or passport authorities in any country? If married, obtain same details on spouse's activities.**

g. ***Item 13 (Employment).*** **Ensure that subject lists all employers, particularly since leaving high school. This includes part–time employment while in school or in the military. All periods of unemployment since high school should be indicated. Has subject had any difficulties with any employment, with employers, supervisors, or coworkers? Has subject been fired or asked to resign? Has subject ever applied for employment with another Federal agency or received any security processing? Has subject ever left an employment knowing he or she was going to be terminated for cause? Has subject owned any foreign property, bonds, stocks, or foreign land, and does subject have any foreign business connections? Has subject ever worked for any foreign government, company, organization, or person?**

h. ***Item 14 (Credit and Character Reference).*** **Has subject ever had any credit difficulties, to include bad checks, collections, repossessions, delinquent accounts, suits, judgments, bankruptcies or liens? Does subject pay obligations on time? Does subject anticipate financial difficulties in the future? If subject's financial system requires it, obtain a complete and current financial status, to include income and expenses, with a listing to each creditor.**

i. ***Item 15 (Residences).*** **Ensure that subject lists actual places of residence during the last 15 years; in particular, ensure that actual residences while in the military are listed. Has subject ever experienced any difficulties with neighbors, landlords, roommates, or members of the military with whom he or she has resided? Pay particular attention to single military personnel. Organization assigned to on post must be listed (for example, Headquarters and Headquarters Company 100th Infantry Div., on post Ft. George). Ask if anyone would attempt to discredit subject in the course of a background investigation.**

j. ***Item 16 (Membership in Organizations).*** **Verify all organizations (one of the most neglected items on SPH: care must be taken). Disregard, however, routine religious–affiliated activities or school athletic organizations. Ensure that all organizations of which subject is, or has been a member are listed. In particular, question subject regarding any membership in foreign organizations. Ensure that any apparently questionable organizations are discussed in detail with subject, particularly any connection or involvement with organizations which resort to illegal means to further their goals.**

k. ***Item 17 (Communist, Fascist or Other Organizations).*** **Has subject or any member of his or her family ever been a member of Communist, Fascist, or subversive organizations? Has subject ever knowingly associated with anyone who, to the subject's knowledge, is a member of the above organizations? Has subject attended meetings of the above organizations, subscribed to their publications, or contributed to them? Has subject ever participated in any demonstration, either illegal or against the U.S. Government? Check—**

(1) **Membership in or sympathetic association with the above.**

(2) **Any type of involvement with any group, movement, or combination, or persons that advocate any of the following:**

(a) **Violent overthrow of the U.S. Government, or**

(b) **Its unconstitutional altering.**

(3) **Any contributions of time, money, or talent to any such organization.**

(4) **Any actions in official capacity, such as agent, officer, or organizer.**

(5) **Any participation in activities, such as meetings, rallies, distribution of handbills or leaflets, picketing, marches, and demonstrations.**

(6) **Any past or present association with any persons, to include relatives, whom the subject has reason to believe may be engaged in some subversive activity.**

(7) **Any incident or circumstances that could possibly reflect adversely on subject's loyalty to the United States.**

(8) **Any actions taken to hinder or prevent persons from exercising their rights under the U.S. Constitution.**

l. ***Item 18 (Criminal Proceeding/Law Enforcement Agencies).*** **Has subject ever been arrested,detained,questioned,interrogated, held,or taken into custody by any law enforcement agency? Has subject ever appeared in court for any reason? Has subject ever been sued by anyone? Has subject ever received a traffic violation in which the total cost to him or her exceeded $100? Ensure that all incidents of unfavorable involvement with law enforcement agencies as an adult or juvenile are covered. Ensure that all Articles 15, captain masts, and courts–martial during any period of subject's military service are covered.**

(1) **Check for the following:**

(a) **For civilian personnel: arrested, detained, held, and so forth; defendant in civil or criminal court; traffic citations (although not required to list those under $100, subject may have numerous citations that show irresponsibility and disregard for the law; any reason why subject's name might appear in any police files.**

(b) **For military personnel: same as above, plus the requirement to list in this section any military offenses developed from Item 8.**

(2) **Ask subject to explain any incident or circumstances in his or her life that could—**

(a) **Make him or her vulnerable to coercion or blackmail.**

(b) **Place him or her in an embarrassing position where pressure could be brought to bear on him or her.**

m. ***Item 19 (Incidents).*** **Solicit information on any incident, condition, or other fact that might negatively affect the subject's character, reliability, suitability, trustworthiness, or loyalty. Examples are: homosexuality, bankruptcies, bad debts, ommission of any material facts, dishonest conduct, and so forth.**

Note: Before accomplishing the above, it is suggested that subject be given a short explanation of the scope and thoroughness of the SBI and be made aware of the opportunity to explain any unfavorable incidents that, if found during the course of the SBI, could adversely affect final clearance action.

n. **Regarding all of the foregoing:**

(1) **If you receive a positive reaction to a question, explore it to the extent that you are satisfied that no additional information exists that could further enhance an understanding of the incident.**

(2) **Remember to use and answer the six basic interrogatives—who, what, when, why, where, and how, particularly in exploring difficult and important items.**

G–8. Types of questions regarded as improper or irrelevant in security investigations unless relevancy to the investigation is established

a. ***Religious matters.***

(1) **Do you believe in God?**

(2) **What is your religious preference or affiliation?**

(3) **Are you anti–Semitic, anti–Catholic or anti–Protestant?**

(4) **Are you an atheist or an agnostic?**

(5) **Do you believe in the doctrine of separation of church and state?**

b. ***Racial matters.***

(1) **What are your views on racial matters, such as desegregation of public schools, hotels, or eating places?**

(2) **Do you entertain members of other races in your home?**

(3) **What are your views on racial intermarriage?**

(4) **Do you believe one race is superior to another?**

c. ***Personal and domestic matters.***

(1) **How much income tax do you pay?**

(2) **What is the source and size of your income?**

(3) **What is your net worth?**

(4) **What contributions do you make to political, charitable, religious, or civic organizations?**

(5) **Describe any physical ailments or diseases you may have.**

(6) **Do you have any serious marital or domestic problems?**

(7) **Are you or have you been a member of a trade union?**

(8) **Is there anything in your past life that you would not want your spouse to know?**

(9) **Have you ever written letters to Senators or Congressman expressing dissatisfaction with the military establishment?**

(10) **Do you feel that you are a person that could be easily persuaded into doing things?**

d. ***Political matters.***

(1) **In political matters, do you consider yourself to be a liberal or a conservative?**

(2) **Are you registered to vote in primary election?**

(3) **Did you vote in the last national, State, or municipal election?**

(4) **Are you a member of a political club or party?**

(5) **Have you ever signed a political petition? Explain**.

(6) **Do you write your Congressman or Senator about issues in which you are interested, or to obtain assistance?**

(7) **What are your views regarding the decisions of the Supreme Court (for example, prayer in public schools, desegregation, and Communist Party cases)?**

(8) **What are your views on the constitutionality of proposed or existing legislation?**

(9) **Do you favor one of the two major political parties in the United States?**

(10) **Do you believe that the present system of Government in the United States is the ideal system for the American people?**

(11) **What are your views on the possibility of disarmament in this day and age?**

(12) **Do you believe that there is a possibility all countries could disband their Armed Forces?**

Appendix H
List of Designated Countries

Table H–1
List of designated countries*

Country or area	Approximate control date
Afghanistan	April 1978
Albania	January 1946
Angola	November 1975
Berlin (Soviet Sector)	April 1946
Bulgaria	October 1946
Cambodia (Kampuchea)	April 1975
China (Peoples' Republic of [includes Tibet!)	October 1949
Cuba	December 1960
Czechoslovakia	February 1948
Estonia	June 1940
Ethiopia	September 1974
German Democratic Republic (East Germany)	April 1946
Hungarian People's Republic (Hungary)	June 1947
Iran	February 1978
Iraq	July 1958
Democratic People's Republic of Korea (North Korea)	September 1945
Laos	June 1977
Latvia	June 1940
Libyan Arab Republic	September 1969
Lithuania	June 1940
Mongolian People's Republic (Outer Mongolia)	
Nicaragua	July 1979
Poland	February 1947
Rumania	December 1947
Southern Yemen	June 1969
Syria	February 1958
Union of Soviet Socialist Republics	October 1922
Democratic Republic of Vietnam (North Vietnam)	December 1946
South Vietnam	April 1975
Yugoslavia	November 1945
Kurile Islands and South Sakhalin (Karafuto)	September 1945

Legend for Table H-1:
*See appendix G, DoD C–5102.21–M–1.

Appendix I
Adjudication Policy

I–1. General

a. The following adjudication policy has been developed to assist DOD adjudicators in making determinations with respect to an individual's eligibility for employment or retention in sensitive duties or eligibility for access to classified information. Adjudication policy relative to access to sensitive compartmented information is contained in DCID 1/14 (reference (1)).

b. While reasonable consistency in reaching adjudicative determinations is desirable, the nature and complexities of human behavior preclude the development of a single set of guidelines or policies that is equally applicable in every personnel security case. Accordingly, the following adjudication policy is not intended to be interpreted as inflexible rules of procedure. The following policy requires dependence on the adjudicator's sound judgment, mature

thinking, and careful analysis as each case must be weighed on its own merits, taking into consideration all relevant circumstances, and prior experience in similar cases as well as the guidelines contained in the adjudication policy, which have been compiled from common experience in personnel security determinations.

c. Each adjudication is to be an overall common sense determination based upon consideration and assessment of all available information, both favorable and unfavorable, with particular emphasis being placed on the seriousness, recency, frequency, and motivation for the individual's conduct; the extent to which conduct was negligent, willful, voluntary, or undertaken with knowledge of the circumstances or consequences involved; and, to the extent that it can be estimated, the probability that conduct will or will not continue in the future. The listed "Disqualifying Factors" and "Mitigating Factors" in this set of Adjudication Policies reflect the consideration of those factors of seriousness, recency, frequency, motivation, etc., to common situations and types of behavior encountered in personnel security adjudications, and should be followed whenever an individual case can be measured against this policy guidance. Common sense may occasionally necessitate deviations from this policy guidance, but such deviations should not be frequently made and must be carefully explained and documented.

d. The "Disqualifying Factors" provided herein establish some of the types of serious conduct under the criteria that can justify a determination to deny or revoke an individual's eligibility for access to classified information, or appointment to or retention in sensitive duties. The "Mitigating Factors" establish some of the types of circumstances that may mitigate the conduct listed under the "Disqualifying Factors." Any determination must include a consideration of both the conduct listed under "Disqualifying Factors" and any circumstances listed under the appropriate or corresponding "Mitigating Factors."

e. The adjudication policy is subdivided into sections appropriate to each of the criteria provided in paragraph 2–200 of this regulation, except 2–200*i*, for which conduct under any of the "Disqualifying Factors" of the adjudication policy or any other types of conduct may be appropriately included if it meets the definition of paragraph 2–200*i*.

f. In all adjudications, the protection of the national security shall be the paramount determinant. In the last analysis, a final decision in each case must be arrived at by applying the standard that the issuance of the clearance or assignment to the sensitive position is "clearly consistent with the interests of national security."

I–2. Loyalty

(See paras 2–200*a*, *b*, *c*, and *d*.)

a. Basis: Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form ofGovernment of the United States by unconstitutional means. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Furnishing a representative of a foreign government information or data which could damage the national security of the United States.

(2) Membership in an organization that has been characterized by the Department of Justice as one which meets the criteria in the above–cited "Basis."

(3) Knowing participation in acts that involve force or violence or threats of force or violence to prevent others from exercising their rights under the Constitution or to overthrow or alter the form of government of the United States or of any State.

(4) Monetary contributions, service, or other support of the organization defined in "Basis," above, with the intent of furthering the unlawful objectives of the organization.

(5) Participation, support, aid, comfort, or sympathetic association with persons, groups, or organizations involved in terrorist activities, threats, or acts.

(6) Evidence of continuing sympathy with the unlawful aims and objectives of such an organization, as defined in the "Basis" above.

(7) Holding a position of major doctrinal or managerial influence in an organization as defined in the "Basis" above.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) Lack of knowledge or understanding of the unlawful aims of the organization.

(2) Affiliation or activity occurred during adolescent/young adult years (17–25), more than 5 years has passed since affiliation was served, and affiliation was due to immaturity.

(3) Affiliation for less than a year out of curiosity or academic interest.

(4) Sympathy or support limited to the lawful objectives of the organization.

I–3. Foreign preference

(See para 2–200*f*.)

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

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) The active maintenance of dual citizenship, by one or more of the following:

(a) Possession of a passport issued by a foreign nation and use of this passport to obtain legal entry into any sovereign state in preference to use of a U.S. passport.

(b) Military service in the armed forces of a foreign nation or the willingness to comply with an obligation to so serve, or the willingness to bear arms at any time in the future on behalf of the foreign state.

(c) Exercise or acceptance of rights, privileges, or benefits offered by the foreign state to its citizens (e.g., voting in a foreign election; receipt of honors or titles; financial compensation due to employment/retirement, educational or medical or other social welfare benefits) in preference to those of the United States.

(d) Travel to or residence in the foreign state for the purpose of fulfilling citizenship requirements or obligations.

(e) Maintenance of dual citizenship to protect financial interests, to include property ownership or employment or inheritance rights in the foreign state.

(f) Registration for military service or registration with a foreign office, embassy, or consulate to obtain benefits.

(2) Employment as an agent or other official representative of a foreign government, or seeking or holding political office in a foreign state.

(3) Use of a U.S. Government position of trust or responsibility to influence decisions in order to serve the interests of another government in preference to those of the United States.

c. Mitigating factors (circumstances which may mitigate disqualifyinginformation):

(1) Claim of dual citizenship is with a foreign country whose

interests are not inimical to those of the United States and is based solely on applicant's or applicant's parent(s)' birth, the applicant has not actively maintained citizenship in the last 10 years and indicates he or she will not in the future act so as to pursue this claim.

(2) Military service while a U.S. citizen was in the armed forces of a state whose interests are not inimical to those of the United States and such service was officially sanctioned by U.S. authorities.

(3) Employment is as a consultant only and service provided is of the type sanctioned by the U.S. Government.

I–4. Security responsibility safeguards

(See paras 2–200*g* and *e*.)

a. Basis: Disregard of public laws, statutes, Executive orders, or regulations, including violation of security regulations or practices, or unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by statute, Executive order, or regulation.

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Deliberate or reckless disregard of security regulations, public laws, statutes, or Executive orders which could have resulted in the loss or compromise of classified information.

(2) Deliberate or reckless violations of security regulations, including, but not limited to, taking classified information home or carrying classified data while in a travel status without proper authorization, intentionally copying classified documents in order to obscure classification markings, disseminating classified information to cleared personnel who have no "need to know," or disclosing classified information or other information, disclosure of which is prohibited by statute, Executive order, or regulation, to persons who are not cleared or authorized to receive it.

(3) Pattern of negligent conduct in handling or storing classified documents.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) Violation of security procedures was directly caused or significantly contributed to by an improper or inadequate security briefing, provided the individual reasonably relied on such briefing in good faith.

(2) Individual is personally responsible for a large volume of classified information and the violation was merely administrative in nature.

(3) Security violation was merely an isolated incident not involving deliberate or reckless violation of security policies, practices, or procedures.

I–5. Criminal conduct

(See para 2–200*h*.)

a. Basis: Criminal or dishonest conduct. When it is determined that an applicant for a security clearance, or a person holding a clearance, has engaged in conduct which would constitute a felony under the laws of the United States, the clearance of such person shall be denied or revoked unless it is determined that there are compelling reasons to grant or continue such clearance. Compelling reasons can only be shown by clear and convincing evidence of the following:

(1) The felonious conduct (a) did not involve an exceptionally grave offense; (b) was an isolated episode; and (c) the individual has demonstrated trustworthiness and respect for the law over an extended period since theoffense occurred; or

(2) The felonious conduct (a) did not involve an exceptionally grave offense; (b) was an isolated episode; (c) was due to the immaturity of the individual at the time it occurred; and (d) the individual has demonstrated maturity, trustworthiness, and respect for the law since that time; or

(3) In cases where the individual has committed felonious conduct but was not convicted of a felony, there are extenuating circumstances which mitigate the seriousness of the conduct such that it does not reflect a lack of trustworthiness or respect for the law. The above criteria supersede all criteria previously used to adjudicate criminal conduct involving commission of felonies under the laws of the United States. Involvement in criminal activities which does not constitute a felony under the laws of the United States shall be evaluated in accordance with the criteria set forth below. (For purposes of this paragraph, the term "felony" means any crime punishable by imprisonment for more than a year. The term "exceptionally grave offense" includes crimes against the Federal Government, its instrumentalities, officers, employees, or agents; or involves dishonesty, fraud, bribery, or false statement; or involves breach of trust or fiduciary duty; or involves serious threat to life or public safety.)

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Criminal conduct involving:

(a) Commission of a State felony.

(b) Force, coercion, or intimidation.

(c) Firearms, explosives, or other weapons.

(d) Dishonesty or false statements, e.g., fraud, theft, embezzlement, falsification of documents or statements.

(e) Obstruction or corruption of Government functions.

(f) Deprivation of civil rights.

(g) Violence against persons.

(2) Criminal conduct punishable by confinement for 1 year or more.

(3) An established pattern of criminal conduct, whether the individual was convicted or not.

(4) Failure to complete a rehabilitation program resulting from disposition of a criminal proceeding or violation of probation, even if the violation did not result in formal revocation of probation. Rehabilitation should not be considered a success or failure while the individual is still on parole/probation.

(5) Criminal conduct that is so recent in time as to preclude a determination that recurrence is unlikely.

(6) Close and continuing association with persons known to the individual to be involved in criminal activities.

(7) Criminal conduct indicative of a serious mental aberration, lack of remorse, or insufficient probability of rehabilitative success (e.g., spouse or child abuse).

(8) *Disposition:*

(a) Conviction.

(b) Disposition on a legal issue not going to the merits of the crime.

(c) Arrest or indictment pending trial when there is evidence that the individual engaged in the criminal conduct for which arrested or indicted.

(9) *Arrest record.* In evaluating an arrest record, information that indicates that the individual was acquitted, that the charges were dropped or the subject of a "stet" or "nolle prosequi," that the record was expunged, or that the cause was dismissed due to error not going to the merits does not negate the security significance of the underlying conduct. Personnel security determinations are to be made on the basis of all available information concerning a person's conduct and actions rather than the legal outcome of a criminal proceeding.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) Immaturity attributable to the age of the individual at the time of the offense.

(2) Extenuating circumstances surrounding the offense.

(3) Circumstances indicating that the actual offense was less serious than the offense charged.

(4) Isolated nature of the conduct.

(5) Conduct occurring only in the distant past (such as more than 5 years ago) in the absence of subsequent criminal conduct.

(6) Transitory conditions directly or significantly contributing to the conduct (such as divorce action, death in family, severe provocation) in the absence of subsequent criminal conduct.

I–6. Mental or emotional disorders

(See para 2–200*j*.)

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

b. Disqualifying factors (behavior or condition falls within one or more of the following categories):

(1) Diagnosis by competent medical authority (board–certified psychiatrist or clinical psychologist) that the individual has an illness or mental condition which may result in a significant defect in judgment or reliability.

(2) Conduct or personality traits that are bizarre or reflect abnormal behavior or instability even though there has been no history of mental illness or treatment, but which nevertheless, in the opinion of competent medical authority, may cause a defect in judgment or reliability.

(3) A diagnosis by competent medical authority that the individual suffers from mental or intellectual incompetence or mental retardation to a degree significant enough to establish or suggest that the individual could not recognize, understand, or comprehend the necessity of security regulations, or procedures, or that judgment or reliability are significantly impaired, or that the individual could be influenced or swayed to act contrary to the national security.

(4) Diagnosis by competent medical authority that an illness or condition that had affected judgment or reliability may recur even though the individual currently manifests no symptoms, or symptoms currently are reduced or in remission.

(5) Failure to take prescribed medication or participate in treatment (including followup treatment or aftercare), or otherwise failing to follow medical advice relating to treatment of the illness or mental condition.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) Diagnosis by competent medical authority that an individual's previous mental or emotional illness or condition that did cause significant defect in judgment or reliability is cured and has no probability of recurrence, or such a minimal probability of recurrence as to reasonably estimate there will be none.

(2) The contributing factors or circumstances which caused the bizarre conduct or traits, abnormal behavior, or defect in judgment and reliability have been eliminated or rectified, there is a corresponding alleviation of the individual's condition and the contributing factors or circumstances are not expected to recur.

(3) Evidence of the individual's continued reliable use of prescribed medication for a period of at least 2 years without recurrence and testimony by competent medical authority that continued maintenance of prescribed medication is medically practical and likely to preclude recurrence of the illness or condition affecting judgment or reliability.

(4) There has been no evidence of a psychotic condition, a serious or disabling neurotic disorder, or a serious character or personality disorder for the past 10 years.

I–7. Foreign connections/vulnerability to blackmail or coercion

(See para 2–200*k*.)

a. Basis: Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be (1) the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States, or (2) any other circumstances that could cause the applicant to be vulnerable.

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Indications that the individual now is being blackmailed, pressured, or coerced by any individual, group, association, organization, or government.

(2) Indications that a vulnerable individual actually has been targeted and/or approached for possible blackmail, coercion, or pressure by any individual, group, association, organization, or government.

(3) Indications that the individual has acted to increase the vulnerability for future possible blackmail, coercion, or pressure by any individual, group, association, organization, or governments, especially by or in a country designated hostile to the United States (see app H). Indicators include, but are not limited to, the following:

(a) Failure to report to security officials any evidence, indication, or suspicion that mail to relatives has been opened, unusually delayed or tampered with in any way, or that telephone calls have been monitored.

(b) An increase in curiosity or official or quasi–official inquiries about the individual to relatives in the country where they reside occasioned by the receipt of mail, packages, telephone calls, or visits from the individual.

(c) Contact with, or visits by, officials to the individual while visiting relatives in another country, to learn more about the individual or the individual's employment or residence, etc.

(d) Unreported attempts to obtain classified or other sensitive information or data by representatives of a foreign country.

(4) Conduct or actions by the individual while visiting in a country hostile to the United States that increase the individual's vulnerability to be targeted for possible blackmail, coercion, or pressure. These include, but are not limited to the following:

(a) Violation of any laws of the foreign country where relatives reside during visits or through mailing letters or packages (e.g., smuggling, currency exchange violations, unauthorized mailings, violations of postal regulations of the country, or any criminal conduct, including traffic violations) which may call the attention of officials to the individual.

(b) Frequent and regular visits, correspondence, or telephone contact with relatives in the country where they reside, increasing the likelihood of official notice.

(c) Failure to report to security officials those inquiries by friends or relatives for more than a normal level of curiosity concerning the individual's employment, sensitive duties, military service, or access to classified information.

(d) Repeated telephone or written requests to the foreign government officials for official favors, permits, visas, travel permission, or similar requests which increase the likelihood of official notice.

(e) Reckless conduct, open or public misbehavior or commission of acts contrary to local customs or laws, or which violate the mores of the foreign country and increase the likelihood of official notice.

(f) Falsification of documents, lying to officials, harassing or taunting officials or otherwise acting to cause an increase in the likelihood of official notice or to increase the individual's vulnerability because personal freedom could be jeopardized.

(g) Commission of any illicit sexual act, drug purchase or use, drunkenness, or similar conduct which increases the likelihood of official notice, or which increases the individual's vulnerability because personal freedom could be jeopardized.

(5) Conduct or actions by the individual that increase the individual's vulnerability to possible coercion, blackmail, or pressure, regardless of the country in which it occurred, including, but not limited to, the following:

(a) Concealment or attempts to conceal from an employer prior unfavorable employment history, criminal conduct, mental or emotional disorders or treatment, drug or alcohol use, sexual preference, or sexual misconduct described under that section below, or fraudulent credentials or qualifications for employment.

(b) Concealment or attempts to conceal from immediate family members, close associates, supervisors, or coworkers, any criminal conduct, mental or emotional disorders or treatment, drug or alcohol abuse, sexual preference, or sexual misconduct described under that section below.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) The individual:

(a) Receives no financial assistance from and provides no financial assistance to persons or organizations in the designated country.

(b) Has been in the United States for at least 5 years since becoming a U.S. citizen without significant contact with persons or organizations from the designated country (each year of active service in the U.S. military may be counted).

(c) Has close ties of affection to immediate family members in the United States.

(d) Has adapted to the lifestyle in the United States, established substantive financial or other associations with U.S. enterprises or community activities.

(e) Prefers the way of life and form of government in the United States over the other country.

(f) Is willing to defend the United States against all threats, including the designated country in question.

(g) Has not divulged the degree of association with the U.S. Government or access to classified information to individuals in the designated country in question.

(h) Has not been contacted or approached by anyone or any organization from a designated country to provide information or favors, or to otherwise act for a person or organization in the designated country in question.

(i) Has promptly reported to proper authorities all attempted contacts, requests, or threats from persons or organizations from the designated country.

(j) Is aware of the possible vulnerability to attempts of blackmail or coercion and has taken positive steps to reduce or eliminate such vulnerability.

I–8. Financial matters

(See para 2–200*l*.)

a. Basis: Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) History of bad debts, garnishments, liens, repossessions, unfavorable judgments, delinquent or uncollectible accounts or debts written off by creditors as uncollectible losses with little or no apparent or voluntary effort by the individual to pay amounts owed.

(2) Bankruptcy due to financial irresponsibility, or with continuing financial irresponsibility thereafter.

(3) Indebtedness aggravated or caused by gambling, alcohol, drug abuse, or other factors indicating poor judgment or financial irresponsibility.

(4) A history or pattern of living beyond the person's financial means or ability to pay, a lifestyle reflecting irresponsible expenditures that exceed income or assets, or a history or pattern of writing checks not covered by sufficient funds or on closed accounts.

(5) Indication of deceit or deception in obtaining credit or bank accounts, misappropriation of funds, income tax evasion, embezzlement, fraud, or attempts to evade lawful creditors.

(6) Indifference to or disregard of financial obligations or indebtedness or intention not to meet or satisfy lawful financial obligations or when present expenses exceed net income.

(7) Unexplained affluence or income derived from illegal gambling, drug trafficking or other criminal or nefarious means.

(8) Significant unexplained increase in an individual's net worth.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) Scheduled program or systematic efforts demonstrated over a period of time (generally 1 year) to satisfy creditors, acknowledge debts, and arrange for reduced payments; entry into debt–consolidation program; or seeking the advice and assistance of financial counselors or court–supervised payment program.

(2) Change to a more responsible life–style, reduction of credit card accounts, and favorable change in financial habits over a period of time (generally 1 year).

(3) Stable employment record and favorable financial references.

(4) Unforeseen circumstances beyond the individual's control (e.g., a major or catastrophic illness or surgery, accidental loss of property or assets not covered by insurance, decrease or cutoff of income, indebtedness resulting from court judgments not due to the individual's financial mismanagement), provided the individual demonstrates efforts to respond to the indebtedness in a reason–able and responsible fashion.

(5) Indebtedness due to failure of legitimate business efforts or business–related bankruptcy without evidence of fault or financial irresponsibility on the part of the individual, irresponsible mismanagement of an individual's funds by another who had fiduciary control or access to them without the individual's knowledge, loss of assets as a victim of fraud or deceit, or debts caused by catastrophic medical expenses not covered by insurance, provided the individual demonstrates efforts to respond to the indebtedness in a reasonable and responsible fashion.

(6) Any significant increase in net worth was due to legitimate business interests, inheritance, or similar legal explanation.

I–9. Alcohol abuse

(See para 2–200*m*.)

a. Basis: Habitual or episodic use of intoxicants to excess.

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Habitual or episodic consumption of alcohol to the point of impairment or intoxication.

(2) Alcohol–related incidents such as traffic violations, fighting, child or spouse abuse, nontraffic violation, or other criminal incidents related to alcohol use.

(3) Deterioration of the individual's health or physical or mental condition due to alcohol use or abuse.

(4) Drinking on the job, reporting for work in an intoxicated or "hungover" condition, tardiness or absences caused by or related to alcohol abuse, and impairment or intoxication occurring during, and immediately following, luncheon breaks.

(5) Refusal or failure to accept counseling or professional help for alcohol abuse or alcoholism.

(6) Refusal or failure to follow medical advice relating to alcohol abuse treatment or to abstain from alcohol use despite medical or professional advice.

(7) Refusal or failure to significantly decrease consumption of alcohol or to change lifestyle and habits which contributed to past alcohol–related difficulties.

(8) Indications of financial or other irresponsibility or unreliability caused by alcohol abuse, or discussing sensitive or classified information while drinking.

(9) Failure to cooperate in or successfully complete a prescribed regimen of an alcohol abuse rehabilitation program.

(10) Failure to continue to abstain from use or abuse of alcohol after successful completion of an alcohol rehabilitation program.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) Successfully completed an alcohol awareness program following two or less alcohol–related incidents and has significantly reduced alcohol consumption, and made positive changes in lifestyle and improvement in job reliability.

(2) Successfully completed an alcohol rehabilitation program after three or more alcohol–related incidents, has significantly reduced or eliminated alcohol consumption in accordance with medical or professional advice, regularly attended Alcoholics Anonymous or similar support organization for approximately 1 year after rehabilitation, and abstained from the use of alcohol for that period of time.

(3) Whenever one of the situations listed below occurs, the individual must have successfully completed an alcohol rehabilitation or detoxification program and totally abstained from alcohol for a period of approximately 2 years:

(a) The individual has had one previously failed rehabilitation program and subsequent alcohol abuse or alcohol–related incidents.

(b) The individual has been diagnosed by competent medical or health authority as an alcoholic, alcoholic dependent, or chronic abuser of alcohol.

(4) Whenever the individual has had repeated unsuccessful rehabilitation efforts and has continued drinking or has been involved in

additional alcohol–related incidents, then the individual must have successfully completed an alcohol rehabilitation or detoxification program, totally abstained from alcohol for a period of at least 3 years, and maintained regular and frequent participation in meetings of Alcoholics Anonymous or similar organizations.

(5) If an individual's alcohol abuse was surfaced solely as a result of self–referral to an alcohol abuse program and there have been no precipitating factors such as alcohol–related arrests or incidents action, will not normally be taken to suspend or revoke security clearance solely on the self–referral for treatment.

I–10. Drug abuse

(See para 2–200*n*.)

a. Basis: Illegal or improper use, possession, transfer, sale, or addiction to any controlled or psychoactive substance, narcotic,[1] cannabis,[2] or other dangerousdrug.[3] **(See table I–1 for a list of drugs designated as controlled substances.)**

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Abuse of cannabis only, not in combination with any other substance.

(a) Experimental abuse, defined as an average of once every 2 months or less, but no more than six times.

(b) Occasional abuse, defined as an average of not more than once a month.

(c) Frequent abuse, defined as an average of not more than once a week .

(d) Regular abuse, defined as an average of more than once a week.

(e) Compulsive use, habitual use, physical or psychological dependency, or use once a day or more on the average.

(2) Abuse of any narcotic, psychoactive substance, or dangerous drug (to include prescription drugs), either alone, or in combination with another or cannabis, as follows:

(a) Experimental abuse, defined as an average of once every 2 months or less, but no more than six times.

(b) Occasional abuse, defined as an average of not more than once a month.

(c) Frequent abuse, defined as an average of not more than once a week.

(d) Regular abuse, defined as an average of more than once a week.

(e) Compulsive use, habitual use, physical or psychological dependency, or use on an average of once a day or more on the average.

(3) Involvement to any degree in the unauthorized trafficking, cultivation, processing, manufacture, sale, or distribution of any narcotic, dangerous drug, or cannabis or assistance to those involved in such acts whether or not the individual was arrested for such activity.

(4) Involvement with narcotics, dangerous drugs, or cannabis under the following conditions whether or not the individual engages in personal use:

(a) Possession.

(b) Possession of a substantial amount, more than could reasonably be expected for personal use.

(c) Possession of drug paraphernalia for cultivating, manufacturing, or distributing (e.g., possession of gram scales, smoking devices, needles for injecting intravenously, empty capsules, or other drug production chemical paraphernalia).

(d) Possession of personal drug paraphernalia such as needles for injecting, smoking devices and equipment, etc.

(5) Information that the individual intends to continue to use (regardless of frequency) any narcotic, dangerous drug, or cannabis. There is no corresponding mitigating factor for this disqualifying factor because it is DOD policy that, as a general rule, if any individual expresses or implies any intent to continue use of any narcotic, dangerous drug, or other controlled substance, including marijuana and hashish, without a prescription, in any amount and regardless of frequency, it is to be considered contrary to the national interest and the interests of national security to grant or allow retention of a security clearance for access to classified information for that individual.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) Abuse of cannabis only. (Use this to assess disqualifying factor 1.)

(a) Experimental abuse occurred more than 6 months ago, and the individual has demonstrated an intent not to use cannabis or any other narcotic, psychoactive substance or dangerous drug in the future.

(b) Occasional abuse of cannabis occurred more than 12 months ago, and the individual has demonstrated an intent not to use cannabis or any other narcotic, dangerous drug, or psychoactive substance in the future.

(c) Frequent abuse of cannabis occurred more than 18 months ago, and the individual has demonstrated an intent not to use cannabis or any other narcotic, dangerous drug, or psychoactive substance in the future.

(d) Regular abuse of cannabis occurred more than 2 years ago, and the individual has demonstrated an intent not to use cannabis or any other narcotic, dangerous drug, or psychoactive substance in the future.

(e) Compulsive, habitual use or physical or psychological dependency on cannabis occurred more than 3 years ago, the individual has demonstrated an intent not to use cannabis or any other narcotic, dangerous drug or psychoactive substance in the future and has demonstrated a stable lifestyle, with no indication of physical or psychological dependence.

(2) Abuse *other than* cannabis alone. Use is considered cumulative and each separate substance must not be considered separately. (Use this to assess disqualifying factor 2.)

(a) Experimental abuse occurred more than 12 months ago, the individual has demonstrated an intent not to use any drugs or cannabis in the future and has successfully completed a drug rehabilitation program.

(b) Occasional abuse occurred more than 2 years ago, the individual has demonstrated an intent not to use any drugs or cannabis in the future, has a stable lifestyle and satisfactory employment record and has successfully completed a drug rehabilitation program.

(c) Frequent abuse occurred more than 3 years ago, the individual has demonstrated an intent not to use any drugs or cannabis in the future, has a stable lifestyle, including satisfactory employment record with no further indication of drug abuse, and has successfully completed a drug rehabilitation program.

(d) Regular abuse occurred more than 4 years ago, the individual has demonstrated an intent not to use any drugs or cannabis in the future, has a stable lifestyle, including satisfactory employment record with no further indication of drug abuse, and has successfully completed a drug rehabilitation program.

(e) Compulsive abuse occurred more than 5 years ago, the individual has demonstrated an intent not to use any drugs or cannabis in the future, has a stable lifestyle, including satisfactory employment record with no further indication of drug abuse, and has successfully completed a drug rehabilitation program.

(3) Use this only to assess conduct under disqualifying factor 3.

(a) Involvement in trafficking, cultivation, processing, manufacture, sale, or distribution occurred more than 5 years ago, the individual has demonstrated an intent not to do so in the future, and has a stable lifestyle and satisfactory employment record and has not been involved in any other criminal activity.

---

[1] *Narcotic.* Opium and opium derivatives or synthetic substitutes.

[2] *Cannabis.*The intoxicating products of the hemp plant, Cannabis Sativa, including but not limited to marijuana, hashish, and hashish oil.

[3] *Dangerous Drug.* Any of the nonnarcotic drugs which are habit forming or have a potential for abuse because of their stimulant, depressant,or hallucinogenic effect.

(b) Cultivation was for personal use only, in a limited amount for a limited period and the individual has not been involved in similar activity or other criminal activity for more than 3 years and has demonstrated intent not to do so again in the future.

(c) Illegal sale or distribution involved only the casual supply to friends of small amounts (not for profit or to finance a personal supply) and occurred on only a few occasions more than 2 years ago, and the individual has demonstrated an intent not to do so again in the future.

(4) Use this only to assess conduct under disqualifying factor 4 in the corresponding subparagraphs.

(a) No possession of drugs or other criminal activity in the last 2 years.

(b) The individual has not possessed drugs in the last 3 years, has had no other criminal activity in the last 3 years, and has demonstrated an intent not to be involved in such activity in the future.

(c) The individual has not possessed drug paraphernalia used in processing, manufacture, or distribution for the last 5 years, has had no other criminal activity in the last 5 years, and has demonstrated an intent not to be involved in such activity in the future.

(d) The individual has not possessed drug paraphernalia for personal use in the last year, has had no other criminal activity in the last 2 years, and has demonstrated an intent not to be involved in such activity in the future.

Table I–1
Drugs designated as controlled substances

Drugs	Often–prescribed brand names
Narcotics	
Opium	Dover's Powder, Paregoric
Morphine	Morphine
Codeine	Codeine
Heroin	None
Heperidine (Pethidine)	Demerol, Pethadol
Methadon	Dolophine, Methadone, Methadose
Other narcotics	Dilaudid, Leritine Numorphan, Percodan
Depressants	
Chloral Hydrate	Noctoc, Somnos
Barbiturates	Amytal, Butisol, Nembutal, Phenobarbital, Seconal,Tuinal
Glutethimide	Doriden
Methaqualone	Optimil, Parest, Quaalude, Somnafac Sopor Equanil,Librium, Miltown, Serax, Tranxene, Valium
Other depressants	
	Clonopin, Dalmane, Dormate, Noludar, Placydil,Valmid
Stimulants	
Cocaine	Cocaine
Amphetamines	Benzedrine, Biphetamine, Desoxyn, Dexedrine
Phenemetrazine	Preludin
Methylphenidate	Ritalin
Other stimulants	
	Bacarate, Cylert, Didrex, Ionamin, Plegine, Pondimin, Pre–State, Sanorex, Voranil
Hallucinogens	
LSD	None
Mescaline	None
Psilocybin–Psilocyn	None
MDA	None
PCP	Sernylan
Other hallucinogens	None
Cannabis	
Marijuana	None
Hashish	None

Table I–1
Drugs designated as controlled substances—Continued

Drugs	Often–prescribed brand names
Hashish Oil	None

I–11. Falsification

(See para 2–200*o*.)

a. Basis: Any knowing and willful falsification, coverup,concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form, or other representation or device used by the Department of Defense or any other Federal agency.

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Deliberate omission, concealment, falsification, or misrepresentation of relevant and material facts, including, but not limited to, information concerning arrests, drug abuse or treatment, alcohol abuse or treatment, treatment for mental or emotional disorders, bankruptcy, military service information, organizational affiliations, financial problems, employment, foreign travel, or foreign connections from any Personnel Security Questionnaire, Personal History Statement, or similar form used by any Federal agency to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance or access eligibility, or award fiduciary responsibilities.

(2) Deliberately providing false or misleading information concerning any of the relevant and material matters listed above to an investigator, employer, supervisor, security official, or other official representative in connection with application for security clearance or access to classified information or assignment to sensitive duties.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) The information was not relevant or material to reaching a security clearance or access determination.

(2) The falsification was an isolated incident in the distant past (more than 5 years) and the individual subsequently had accurately provided correct information voluntarily during reapplication for clearance or access and there is no evidence of any other falsification, misrepresentation, or dishonest conduct by the individual.

(3) The behavior was not willful.

(4) The falsification was done unknowingly or without the individual's knowledge.

(5) The individual made prompt, good faith efforts to correct the falsification before being confronted with the facts of falsification.

(6) Omission of material fact was caused by or significantly contributed to by improper or inadequate advice of authorized personnel, provided the individual reasonably relied on such improper or inadequate advice in good faith, and when the requirement subsequently was made known to the individual, the previously omitted information was promptly and fully provided.

I–12. Refusal to answer

(See para 2 –200*p*.)

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

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) Failure or refusal to provide full, frank, and truthful answers or to authorize others to do so, in connection with any application for security clearance or access, to include required nondisclosure and security termination agreements.

(2) Failure or refusal to provide appropriate investigative forms,

including release forms, for use by investigators in obtaining information from medical institutions, agencies, or personal physicians, therapists, psychologists, psychiatrists, counselors, rehabilitation treatment, agencies, or personnel, police or criminal agencies, probation agencies or officers, financial institutions, employers, Federal or State agencies, professional associations, or any other organizations as required as part of an investigation for security clearance, access, appointment, or assignment to sensitive duties.

(3) Failure or refusal to authorize others to provide relevant and material information necessary to reach a security clearance determination.

(4) Failure or refusal to answer questions or provide information required by a congressional committee, court, or agency when such answers or information concern relevant and material matters pertinent to evaluating the individual's trustworthiness, reliability, and judgment.

(5) Failure or refusal to submit to psychiatric, psychological, drug, or alcohol evaluation, when necessary to reach a security clearance determination.

c. Mitigating factors (circumstances which may mitigate disqualifying information):

(1) The individual was unable to provide the information despite good faith and reasonable efforts to do so.

(2) The individual was unaware of the necessity to provide the information requested or of the possible consequences of such refusal or failure to provide the information, and, upon being made aware of this requirement, fully, frankly, and truthfully provided the requested information.

(3) The individual sought and relied in good faith on information and advice from legal counsel or other officials that the individual was not required to provide the information requested, and, upon being made aware of the requirement, fully, frankly, and truthfully provided the requested information.

I–13. Sexual misconduct

(See para 2–200*q*.)

a. Basis: Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.

b. Disqualifying factors (behavior falls within one or more of the following categories):

(1) The conduct involves:

(a) Acts performed or committed in open or public places.

(b) Acts performed with a minor, or with animals.

(c) Acts involving inducement, coercion, force, violence, or intimidation of another person.

(d) Prostitution, pandering, or the commission of sexual acts for money or other remuneration or reward.

(e) Sexual harassment.

(f) Self–mutilation, self–punishment, or degradation.

(g) Conduct that involves spouse swapping, or group sex orgies.

(h) Adultery that is recent, frequent, and likely to continue and has an adverse effect on good order or discipline within the workplace (e.g., officer/enlisted, supervisor/subordinate, or instructor/student).

(i) Conduct determined to be criminal in the locale in which it occurred.

(j) Deviant or perverted sexual behavior which may indicate a mental or personality disorder (e.g., transexualism, transvestism, exhibitionism, incest, child molestation, voyeurism, bestiality, or sodomy).

(2) The conduct has been recent.

(3) The conduct increases the individual's vulnerability to blackmail, coercion, or pressure.

(4) Evidence indicates that the applicant has intention or is likely to repeat the conduct in question.

c. Mitigating factors (circumstances which may mitigate qualifying information):

(1) Sexual misconduct occurred on an isolated basis during or preceding adolescence with no evidence of subsequent conduct of a similar nature, and clear indication that the individual has no intention of participating in such conduct in the future.

(2) Sexual misconduct was isolated, occurred more than 3 years ago, and there is clear indication that the individual has no intention of participating in such conduct in the future.

(3) The individual was a minor or was the victim of force or violence by another.

(4) The individual has successfully completed professional therapy, has been rehabilitated and diagnosed by competent medical authority that misconduct is not likely to recur.

(5) Demonstration that the individual's sexual misconduct can no longer form the basis for vulnerability to blackmail, coercion, or pressure.

Appendix J
Overseas Investigations

J–1. Purpose

The purpose of this appendix is to establish, within the framework of this regulation, DOD Directive 5105.42 and Defense Investigative Service 20–1–M, (references (hh) and (ii)) standardized procedures for the military investigative agencies to follow when they perform administrative and investigative functions on behalf of DIS at overseas locations.

J–2. Type investigation

This regulation describes in detail background investigations (BIs) which are conducted for limited access authorizations and those special investigative inquiries conducted for postadjudicative purposes. Hereafter they are referred to as LAA and postadjudicative cases and are briefly described in paragraphs *a* and *b* below:

a. Limited access authorization. A level of access to classified defense information that may be granted to a non–U.S. citizen under certain conditions, one of which is that a BI must have been completed with satisfactory results. Paragraph 3–403 further describes LAA cases.

b. Postadjudication investigation. A personnel security investigation (PSI) predicated on new, adverse, or questionable security, suitability or hostage information that arises and requires the application of investigation procedures subsequent to adjudicative action on a DOD–affiliated person's eligibility for continued access to classified information, assignment to or retention in sensitive duties or other designated duties requiring such investigation. While these cases are normally predicated on the surfacing of unfavorable information subsequent to favorable adjudication, they may also be opened when favorable information is offered to counter a previous unfavorable adjudication. Paragraph 2–402*c* further describes these cases.

J–3. General

a. As a rule, investigative activity in most PSIs occurs in the U.S. even when the subject is at an overseas location. Therefore, the submission of requests for investigation to the Personnel Investigation Center (PIC) at Baltimore is a required procedure as it ensures uniform application of DOD PSI policy and the efficient dispatch and coordination of leads.

b. When the purpose of the investigation is for an LAA or postadjudication on a subject overseas, much, if not all of the leads are at an overseas location. While these cases also may be submitted directly to PIC for action, there is an inherent delay in the mailing of the request, the exchange of leads and reports with PIC, and transmittal of the reports back to the requester. To avoid this delay, the military investigative agencies, when acting for DIS overseas in accordance with DOD Directive 5105.42 (reference (hh)) may, with their headquarters approval, accept these requests for investigations, initiate them and disseminate the results from the same level as they open, close, and disseminate their own cases. Usually this will greatly improve response time to the requester.

c. Under the procedures in paragraph *b*, above, DIS will not often

be in a position to directly exercise its responsibility for control and direction until the case or lead is in progress or even completed; therefore, adherence to the policy stated in referenced documents, and as modified herein, is mandatory. When the policy of the military investigative agency is at variance with the above, the matter will be referred to the respective headquarters for resolution.

d. Since DIS is ultimately responsible for the personnel security product, it must be kept informed of all such matters referred to in this appendix. For instance, when the investigative agency overseas receives a DD Form 1879, Request for Personnel Security Investigation, which sets forth an issue outside DIS jurisdiction, it will reject the request, inform the requester of the reason and furnish an information copy of the DD Form 1879 and rejection letter to PIC. When the issue/jurisdiction is unclear to the investigative agency, the DD Form 1879 and the perceived jurisdictional question should be promptly forwarded to DIS for action and, if appropriate, to the Component's headquarters for information. Questions on the interpretation of DIS or DOD policy and directives pertaining to individual PSI cases can usually be resolved through direct communications with PIC.

e. DOD Directive 5105.42 (reference (hh)), establishes the supporting relationship of the military investigative agencies to DIS in overseas areas, and DIS provides these agencies with copies of relevant policy and interpretive guidance. For these reasons, the investigative agency vice the requester, is responsible for evaluating the request, processing it, collecting and evaluating the results within their jurisdiction for sufficiency, and forwarding the completed product to the appropriate activity.

f. The magnitude of operations at PIC requires that methods of handling LAA and postadjudicative cases be consistent to the maximum extent possible. For this reason, the procedures for LAA cases are nearly identical to those for postadjudicative cases. Briefly, the main exceptions are:

(1) The notification to PIC that a postadjudication case has been opened will be by message, since an issue is present at the outset, whereas notification of an LAA case should normally be by mail.

(2) The scope of the LAA investigation is 10 years or since the person's 18th birthday, whichever is shortest, whereas the leads in a postadjudication case are limited to resolving the issue.

J–4. Jurisdiction

a. As set forth in DOD Directive 5105.42 (reference (hh)), DIS is responsible for conducting all DOD PSIs in the 50 States, District of Columbia, and Puerto Rico, and will request the Military Departments to accomplish investigative requirements elsewhere. The military investigative agencies in overseas locations routinely respond to personnel security investigative leads for DIS.

b. DIS jurisdiction also includes investigation of subversive affiliations, suitability information, and hostage situations when such inquiries are required for personnel security purposes; however, jurisdiction will rest with the military investigative agencies, FBI and/or civil authorities as appropriate when the alleged subversion or suitability issue represents a violation of law or, in the case of a hostage situation, there is an indication that the person concerned is actually being pressured, coerced, or influenced by interests inimical to the United States, or that hostile intelligence is taking action specifically directed against that person. Specific policy guidance on the applicability of these procedures and the jurisdictional considerations are stated in chapter II, section 4.

J–5. Case opening

a. A request for investigation must be submitted by using DD Form 1879 and accompanied by supporting documentation unless such documentation is not immediately available, or the obtaining of documentation would compromise a sensitive investigation. Upon receipt of the request, the military investigative Component will identify the issue(s), scope the leads, and ensure that the proposed action is that which is authorized for DIS as delineated in this regulation, DOD Directive 5105.42, and Defense Investigative Service 20–1–M (references (hh) and (ii)).

b. Upon such determination, the Component will prepare an action lead sheet (ALS) which fully identifies the subject and the scope of the case, and specifies precisely the leads which each investigative component (including DIS/PIC when appropriate) is to conduct.

c. Case–opening procedures described above are identical for LAA and postadjudication cases except with respect to notification of case opening to PIC:

(1) *Postadjudication cases.* These cases, because they involve an issue, are potentially sensitive and must be examined as early as possible by PIC for conformity to the latest DOD policy. Accordingly, the initial notification to PIC of case openings will always be by message. The message will contain at a minimum:

(a) Full identification of the subject;

(b) A narrative describing the allegation/facts in sufficient detail to support opening of the case; and

(c) A brief listing of the leads that are planned. The DD Form 1879 and supporting documents, along with the agency's ALS, should be subsequently mailed to PIC.

(2) *LAA cases.* The notification to PIC of case opening will normally be accomplished by mailing the DD Form 1879, DD Form 398 (Personal History Statement), a copy of the ALS, and any other supporting documents to PIC. Message notification to PIC in LAA cases will only be required if there is a security or suitability issue apparent in the DD Form 1879 or supporting documents.

d. Beyond initial actions necessary to test allegation for investigative merit and jurisdiction, no further investigative action should commence until the notification of case opening to PIC has been dispatched.

e. PIC will promptly respond to the notification of case opening by mail or message specifying any qualifying remarks along with a summary of previously existing data. PIC will also provide a DIS case control number (CCN). This number must be used by all Components on all case–related paperwork/reports.

(The investigating agency may assign its unique service CCN for interim internal control; however, the case will be processed, referenced, and entered into the DCII by the DIS case control number.) The first five digits of the DIS CCN will be the Julian date of the case opening when received at DIS.

J–6. Case processing

a. The expected completion time for leads in LAA cases is 50 calendar days and for postadjudication cases, 30 days, as computed from the date of receipt of the request. If conditions preclude completion in this time period, a pending report of the results to date, along with an estimated date of completion will be submitted to PIC.

b. Copies of all ALSs will be furnished to PIC. In addition, PIC will be promptly notified of any significant change in the scope of the case, or the development of an investigative issue.

c. The procedures for implementing the Privacy Act in PSI cases are set in DIS 20–1–M (reference (ii)). Any other restrictions on the release of information imposed by an overseas source or by regulations of the country where the inquiry takes place will be clearly stated in the report.

d. The report format for these cases will be that used by the military investigative agency.

e. Investigative action outside the jurisdictional area of an investigative Component office may be directed elsewhere by ALS as needed in accordance with that agency's procedures and within the following geographical considerations:

(1) Leads will be sent to PIC if the investigative action is in the United States, District of Columbia, Puerto Rico, American Samoa, The Bahamas, the U.S. Virgin Islands, and the following islands in the Pacific: Wake, Midway, Kwajalin, Johnston, Carolines, Marshalls, and Eniwetok.

(2) Leads to areas not listed above may be dispatched to other units of the investigative agency or even to another military agency's field units if there is an agreement or memorandum of understanding that provides for such action. For case accountability purposes, copies of such "lateral" leads must be sent to the PIC.

(3) Leads that cannot be dispatched as described in subparagraph (2), above, and those that must be sent to a non–DOD investigative agency should be sent to PIC for disposition.

f. The Defense Investigative Service 20–1–M (reference (ii)) calls for obtaining PIC approval before conducting a subject interview on a postadjudicative investigation. To avoid the delay that compliance with this procedure would create, a military investigative Component may conduct the interview provided:

(1) All other investigative leads have been completed and reviewed.

(2) The CCN has been received, signifying DIS concurrence with the appropriateness of the investigation.

(3) Contrary instructions have not been received from the PIC.

(4) The interview is limited to the resolution of the relevant issues disclosed by the investigation.

g. Notwithstanding the provisions of paragraphs *f*(1) through (4), above, if time is of the essence due to imminent transfer of the subject, a subject interview may be conducted at the discretion of the investigative agency.

J–7. Case responsibility LAA and PA

Paragraph **J–**3, above, describes the advantages of timely handling which accrue when the military investigative Components act for DIS overseas. These actions for DIS may, however, be limited by the Component's staffing and resource limitations, especially since some cases require more administration and management than others. Postadjudication case leads, for instance, will normally be within the geographical jurisdiction of the Component that accepted the request for investigation; therefore, relatively little case management is required. In contrast, LAA cases may require leads worldwide, and, therefore, create more complex case management and administration, especially in the tracking, monitoring and reviewing of leads outside the Component's geographical area. Accordingly, an investigative Component will accept the case from the requester, but only assign itself the appropriate leads within its own geographical jurisdiction and send the balance to PIC for appropriate disposition in accordance with the following:

a. The investigative agency will accept the request for investigation (thereby saving time otherwise lost in mailing to PIC) but limit its involvement in case management by extracting only those leads it will conduct or manage locally.

b. The agency should then prepare an ALS that shows clearly what leads it will cover and send PIC a copy of this ALS, along with the request for investigation and any other appropriate documentation. It must be clear in the ALS that PIC is to act on all those leads that the unit has not assigned to itself.

c. PIC, as case manager, will assume responsibility for the complete investigative package and, upon receipt of the last lead, will send the results to the appropriate activity.

d. The agency that accepted the case and assigned itself leads may send a copy of its report to the activity in the "Results to" block at the same time it sends the originals to PIC. If so, the letter of transmittal must inform the recipient that these reports are only a portion of the investigation, and that the balance will be forthcoming from PIC. Similarly, PIC must be informed of which investigative reports were disseminated. (This is normally done by sending PIC a copy of the letter of transmittal.)

J–8. Scope

a. LAA. The scope of investigation is 10 years or from age 18, whichever is the shortest period.

b. Postadjudication cases. There is no standard scope. The inquiries conducted will be limited to those necessary to resolve the issue(s).

J–9. Case closing: LAA and PA

a. Whether the investigative Component or PIC closes out an investigation, there are three key elements to consider:

(1) The investigative results must be reviewed for quality and conformance to policy.

(2) The results must be sent to the activity listed in the "Results to" block of the DD Form 1879.

(3) PIC must be informed whether or not any dissemination was made by the investigative agency and, if so, what reports were furnished.

b. Investigative results may also be sent to a requester or higher level activity that makes a statement of need for the results. In such instances, a copy of the letter requesting the results and the corresponding letter of transmittal must be sent to PIC for retention.

c. When an investigative agency disseminates reports for PIC, it may use the transmittal documents, letters, or cover sheets it customarily uses for its own cases.

d. The material that is to be provided to PIC will consist of: The originals of all reports, and all other case documentation such as original statements, confidential source sheets, interview logs, requests for investigation, letters of transmittal to adjudicators/requesters, or communications with the requester, such as those that modify the scope of the investigation.

e. For DIS to fulfill its responsibilities under DOD 5220.22–R **(AR380–49)** (reference (a)) and the Privacy Act of 1974 (reference (m)), all inquiries conducted in its behalf must be set forth in a Report of Investigation for the permanent file, whether the case is completed, terminated early, or referred to another agency.

J–10. Referral

A case may require premature closing at any time after receipt of the DD Form 1879 by the investigative Component if the information accompanying the request, or that which is later developed, is outside DIS jurisdiction. For example, alleged violations of law, a counterintelligence matter, or actual coercion/influence in a hostage situation (see para **J–**4*b* above) must be referred to the appropriate agency, and DIS involvement terminated. The requester will be informed by letter or endorsement to the DD Form 1879 of the information developed that, due to jurisdictional consideration, the case was referred to (fill in appropriate address) and that the DIS case is closed. The agency to which referral was made and PIC will be furnished with the results of all investigations conducted under DIS auspices. DIS, however, has an interest in the referral agency's actions and no information should be solicited from that agency.

Appendix K
ADP Position Categories and Criteria for Designating Positions

OMB Circular A–71 (and Transmittal Memo #1), July 1978 **(reference (hhh))**, OMB Circular A–130, December 12, 1985 **(reference (iii))**, and FPM Letter 732, November 14, 1978 **(reference (ggg))** contain the criteria for designating positions under the existing categories used in the personnel security program for Federal civilian employees as well as the criteria for designating ADP and ADP–related positions. This policy is outlined below:

K–1. ADP position categories

a. Critical–sensitive positions. ADP–I positions. Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

b. Noncritical–sensitive positions. ADP–II positions. Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP–I category to ensure the integrity of the system.

c. Nonsensitive positions. ADP–III positions. All other positions involved in computer activities.

In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower

categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system.

K–2. Criteria for designating positions

Three categories have been established for designating computer and computer–related positions—ADP–I, ADP–II, and ADP– III. Specific criteria for assigning positions to one of these categories are as follows:

a. ADP–I.

(1) Responsibility for the development and administration of agency computer security programs, including direction and control of risk analysis and/or threat assessment.

(2) Significant involvement in life–critical or mission–critical systems.

(3) Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

(4) Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the ADP–I category to ensure the integrity of the system.

(5) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

(6) Other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

b. ADP–II. Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP–I category, includes, but is not limited to:

(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government–developed privileged information involving the award of contracts;

(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP–I positions.

c. ADP–III. All other positions involved in Federal computer activities.

Appendix L
Defense Security Briefing Provided U.S. Government Employees Traveling to Communist–Controlled Countries

L–1. Introduction

All U.S. Government employees, regardless of position or assignment,are likely to be of interest to intelligence services of Communist–controlled countries. Hostile intelligence networks make it their business to learn the identities of Americans, and frequently try to target them for intelligence approaches when they travel abroad. The approach may be direct or indirect, highly sophisticated or crudely obvious. In any case, U.S. personnel traveling to Communist–controlled countries should be constantly alert to the problems that can befall them. The purpose of this briefing is to make employees aware of pitfalls associated with such travel, and to advise them on defensive measures against hostile intelligence exploitation.

L–2. Before departure

a. **The Bureau of Consular Affairs, U.S. Department of State, frequently publishes advisory material on current travel conditions in Communist–controlled countries. This material should be available through your agency, and you should carefully review any such information covering a country you will be visiting. It is especially important that you are aware of the items that you may or may not take into a country.**

b. **Visa applications are routinely scrutinized by intelligence services of Communist–controlled countries. To avoid difficulties in this area, it is important that you complete the forms truthfully and accurately. It is especially important that you name any relatives that you intend to visit in the host country.**

c. **When obtaining visas, ask the appropriate consular officer how much foreign currency (United States and other) and what valuables you may take into and out of the Communist country or countries to be visited. Make sure you have enough money for the trip, and strictly follow the approved itinerary. You may not import local currency into a country you will be visiting.**

d. **If you are a naturalized American citizen of East European origin, please note that there have been instances in which an East European country has not recognized the U.S. citizenship of former nationals and has taken the position that such persons retain their original nationality and are therefore subject to treatment as citizens of that country upon reentry into its jurisdiction. If this situation applies to you, consult first with the U.S. Department of State for advice and clarification of your status.**

e. **You may wish to carry with you gifts for friends or relatives. Such gifts should be neither controversial nor prohibited. Do not bring pornography, narcotics, or political material. Communist pornography laws are more strict than those in the United States, and you should avoid taking with you magazines or other materials that might be considered pornographic. Any patent medicines or prescription drugs should be clearly for your own use and in quantities reasonable enough to convince authorities that they are for your personal consumption.**

f. **Do not carry with you, on behalf of a third party, any letters, messages, or packages for private individuals in Communist countries. You may be deemed guilty of circumventing normal channels of communication, or you may be regarded as a courier for illegal or subversive purposes.**

g. **Carry only essential forms of identification. Leave Government badges, building passes, and so forth, at home. Write down your passport number and keep it separate from your passport. Do the same with the address and telephone number of the American Embassy.**

h. **DO NOT TAKE THIS DOCUMENT WITH YOU! Study, think about, and remember its warnings during your visit, but leave the document at home.**

L–3. Upon arrival

a. **Rules governing declaration of valuables and currency and those relating to transactions are strictly enforced. Make an accurate declaration at entry of all money and valuables, including travelers checks. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. It is important to keep receipts of all money changes, as these are frequently requested upon departure. Undeclared sums of U.S. or other currency are most likely to cause difficulty with authorities and may be confiscated upon departure.**

b. **You will generally be permitted to take in such items as cameras, transistor radios, and so forth. It is wise to declare such items as you enter, however, to preclude possible explanations, customs charges, or confiscations when you leave. Baggage inspections may be extremely thorough or only perfunctory. On occasion, your baggage may not even be opened at entry.**

c. **As soon as possible after arrival, you should contact the American Embassy or consulate, either by telephone or in person, and provide your local address and the probable length of your visit.**

d. **It is unwise for you to drive in a Communist country. Try to use public transportation or hire a driver, as local traffic regulations may be confusing. There have been incidents when**

traffic accidents were deliberately provoked to incriminate or embarrass a visitor.

L–4. Activities while in Communist countries

a. **Assume that your hotel room is equipped with devices to overhear or record your conversations. There may be devices installed through which you can be physically observed, even while your room is in darkness. In addition to the usual microphones, telephone tapes, miniature recording devices, and so forth, intelligence operatives today use infrared cameras, infrared "snooper–scopes" and optical lenses, closed–circuit TV, and other highly advanced equipment. Do not search for such devices, and do not make an issue of it if you should by chance find one. The presence of such equipment may not necessarily concern you. A device may or may not be monitored during your visit, or it may be monitored only on a "spot check" basis. Do not try to neutralize such a device by running tap water, playing your radio, and so forth. Some modern devices are so sophisticated that they cannot be neutralized. Efforts to combat such penetration will only make the intelligence service more suspicious of you. The best defense against such devices is to keep your conversations light and uninformative.**

IMPORTANT: Should you discover any device of the above kind, take no overt action against it. Continue your normal conversation, giving no indication of your discovery, and report your findings to the American Embassy or consulate or to your security officer upon your return.

b. **Beyond your hotel room, you should assume that conversations in vehicles (including Embassy vehicles), train compartments, restaurants, conference rooms, and other public places may be monitored. Miniature microphones with transmitters or recorders can easily be secreted on the person of an individual in your group. It is even technically possible to record your conversations in open, outdoor areas; however, those areas are normally more secure than indoor locations.**

c. **Avoid unnecessary discussions of your job, your workplace, and other official matters. Also avoid discussing other U.S. employees' habits, character, or other matters that reveal weaknesses or idiosyncrasies.**

d. **Assume that your personal luggage will be searched at some time in your hotel room. If you discover evidence of this, do not make a big issue of it. You should, however, report positive evidence of such activity to the American Embassy and to your security officer upon your return. It is just as well not to bother locking your luggage since most locks will be readily picked. Locked luggage will only increase the curiosity of the intelligence agent and the lock may be broken. Never leave unattended luggage containing valuable papers or documents you do not wish anyone else to read. If you surprise someone searching your possessions, don't take any violent or physical action, but report the incident to local and U.S. authorities.**

e. **You may receive a "wrong number" or otherwise mysterious telephone call in the hotel room at any hour. Do not let this unduly upset you. It may be a crude but effective method of determining whether you are in your room, or it may be only a result of poor telephone service.**

f. **Do not rely on hotel employees for protection service. Assume that they, as well as restaurant employees, are in the employ of the intelligence services. Be particularly circumspect in your relations with guides, interpreters, and Communist travel agency personnel, since these people are invariably used by intelligence agencies.**

g. **You may be under physical surveillance when you travel, whether on foot or in a vehicle. Or you may suspect you are being observed when actually you are not. In either event, the best tactic is to ignore it. Communist intelligence agents at various times observe visitors on a spot check basis for no apparent reason. On the other hand, they may be collecting detailed data concerning your activities in preparation for a more direct intelligence approach. Do not attempt to lose surveillance agents. If you are actually being followed for intelligence objectives, you will be covered by a team of several agents, and your evasion attempts will make them more suspicious.**

h. **You will be permitted to take photographs with your personal camera, but be careful not to photograph restricted areas. You should not take photographs from aircraft, or of military and police installations and personnel, industrial structures, harbors, rail and airport facilities, and border areas. Communist officials also resent your photographing items that put them in a bad light, such as slum areas, public drunks, scenes of civil disorder, or public disturbances. If you do take such photographs, your film may be confiscated.**

i. **Be particularly circumspect in approaches from persons offering social companionship, especially of a sexual nature. Many of these persons are "plants" from Communist intelligence agencies and will attempt to entice you into a compromising situation, which they can use to blackmail you to force your cooperation in intelligence activities. Under no circumstances should you seek or accept this kind of companionship in a Communist country. The intelligence services will capitalize immediately on any indication of immoral or indiscreet behavior of American travelers. Even when failing to detect a vulnerability, Communist agents have attempted to entrap innocent travelers. For this reason, you should maintain the highest level of personal behavior at all times, avoid long walks at night alone, and endeavor always to be in the company of someone you can trust. Be especially careful not to drink too heavily so as not to weaken your defense or lose your self–control.**

j. **Do not accept from anyone (including friends, relatives, or professional contacts) letters, photographs, packages, or any other material to be smuggled out of the country or carried in your effects when you depart. Be firm in your denials in these matters, since such requests may be acts of intelligence agents seeking to entrap you.**

k. **Bear in mind that there are many political, cultural, and legal differences between the United States and Communist countries. Actions that are innocent or, at worst, carry wrist–slapping penalties in the United States, are often considered serious offenses against the law in Communist–dominated societies. Persons violating the law, even unknowingly, run the risk of arrest or expulsion. Do not, for instance, take "souvenirs" from hotels or institutions, however insignificant in value they may appear.**

l. **Do not engage in any private currency transactions with individual citizens. Do not try to sell or trade any personal item, including clothing, which you have brought into the country, or purchase bargains from street peddlers or questionable vendors. Do not engage in black–market activities. Many Communist countries have laws governing exportation of artwork and historic relics. Be familiar with these laws if you intend to purchase such items, and make these purchases only at official establishments.**

m. **Should you be detained or arrested for any reason by police or other officials of these countries, be cooperative, but insist politely and repeatedly, if necessary, that the American Embassy or consulate be notified promptly. Do not make any statements or sign any documents that you do not fully understand until you have had an opportunity to confer with an Embassy representative. You may possibly be accused of having some connection with an American intelligence service or of having accepted an assignment from such service to be carried out in the host country. You should make no admission that you had any dealings, under any circumstances, with any U.S. intelligence agency.**

n. **Mail you receive or send in a Communist country is subject to censorship. In any correspondence before, during, or after your visit, make no reference to classified information nor reveal information of possible value to a hostile intelligence service. Be careful in writing to or about relatives or friends in these**

countries, since they may become targets for investigation or exploitation.

o. **There have been several incidents in Communist countries wherein speech–inducing drugs, medicines, and so forth, have been used to aid in interrogation. In nonemergency situations, make every effort to avoid Communist hospitals or medical facilities without first notifying the American Embassy or consulate.**

p. **Report immediately any attempt to pressure or compromise you, or any action that might lead to such pressure or compromise, to the American Embassy security officer in the country being visited. Report to your security manager immediately if you have unusual subsequent contacts with nationals of a Communist country.**

L–5. Conclusion

This briefing covers many, but not necessarily all, pitfalls that an American traveler may encounter. New espionage techniques and tactics are constantly being developed, and you should always be alert for them. Although the techniques employed by Communist countries' intelligence services may seem farfetched or taken from spy novels, they are in fact used in day–to–day activities and operations. American travelers must recognize that these techniques, however distasteful, are part of the Communist system and be prepared to counter them.

The pitfalls outlined above reflect possibilities, not probabilities, however. You probably will not have any problems if you respect local laws and customs, act honestly in your dealings, and behave discreetly. You can expect friendly treatment from most of the citizens you meet, and you will find that they are very interested in all aspects of American life. You can therefore serve as a valuable goodwill ambassador for the United States while you are traveling in Communist countries. Be open to this experience, have a good trip, and come home safely.

Glossary

Section I
Abbreviations

AA&E
arms, ammunition, and explosives

ADAPCP
Alcohol and Drug Abuse Prevention and Control Program

ADP
automated data processing

ALS
action lead sheet

ARNG
Army National Guard

BI
background investigation

BVS
Bureau of Vital Statistics

CAP
centralized assignment procedure

CCF
U.S. Army Central Clearance Facility

CIA
Central Intelligence Agency

CMF
career management field

DA
Department of the Army

DASEB
DA Suitability Evaluation Board

DCII
Defense Central Index of Investigations

DCIS
Defense Criminal Investigative Service

DCR
developed character reference

DCSINT
Deputy Chief of Staff for Intelligence

DCSPER
Deputy Chief of Staff for Personnel

DDPSS
department–determined personnel security status

DIS
Defense Investigative Service

DISCO
Defense Industrial Security Clearance Office

DNACI
DOD National Agency Check and written inquiries

DOE
Department of Energy

DPOB
date and place of birth

ENTNAC
Entrance National Agency Check

FBI
Federal Bureau of Investigation

HQDA
Headquarters, Department of the Army

INS
Immigration and Naturalization Service

IRR
Individual Ready Reserve

LAA
limited access authorization

LAC
local agency check

LCR
listed character reference

LOI
letter of intent

MACOM
major Army command

MOS
military occupational specialty

MPRJ
Military Personnel Records Jacket

MTOE
modification table of organization and equipment

NAC
National Agency Check

NACI
National Agency Check and written inquiries

NATO
North Atlantic Treaty Organization

NRC
Nuclear Regulatory Commission

NSA
National Security Agency

ODCSPER
Officer of the Deputy Chief of Staff for Personnel

ODUS(P)
Office of the Deputy Under Secretary of Defense for Policy

OJCS
Office of the Joint Chiefs of Staff

OMPF
official military personnel file

OPF
official personnel folder

OPM
Office of Personnel Management

OSS
Office of Strategic Services

PIC
Personnel Investigation Center

PMO
personnel management office

PR
periodic reinvestigation

PRP
Personnel Reliability Program

PSI
personnel security investigation

PSQ
personal security questionnaire

PSSP
Personnel Security Screening Program

ROTC
Reserve Officer Training Corps

SA
Secretary of the Army

SASF
SIDPERS authorized strength file

SBI
special background investigation

SCI
sensitive compartmented information

SIDPERS
Standard Installation/Division Personnel

SII
Special Investigative Inquiry

SIOP–ESI
Single Integrated Operation Plan—extremely sensitive information

SOIC
Senior Officer of the Intelligence Community

SSN
social security number

SSO
special security officer

SPH
statement of personal history

TAADS
The Army Authorization Documents System

TAPA
Total Army Personnel Agency

TDA
tables of distribution and allowances

UCMJ
Uniform Code of Military Justice

USO
United Service Organizations

WHLO, OCSA
White House Liaison Office, Office of the Chief of Staff, Army

Section II
Terms
This sections contains no entries.

Section III
Special Abbreviations and Terms
There are no special terms.

Index

This index is organized alphabetically by topic and subtopic. Topics and subtopics are identified by paragraph number.

Access to chemical agents, 3–610
Access to classified information. *See also* limited access authorization
By Members of Congress, 3–404
By non–U.S. citizens, 2–100, 3–403, appendix F
By persons outside the executive branch, 3–404
By retired General Officers, 3–408
Definition, 1–300
Eligibility for, 6–102, appendix I
Granting, 2–100, 3–605, 7–102
Interim, 8–102
Limiting, 2–501
One–time, 3–407, 3–501
Requires reinvestigation, 3–708
Standards for, 2–100–2–102
Suspension of, 1–327, 8–101, 8–102
Withdrawals of, 7–103
Access to equipment, 3–601
Access to investigative records, 10–102
Access to restricted areas, 3–601
Access to sensitive compartmented information, 2–308, 3–703
Access to TOP SECRET, 3–101, 3–104, 3–703, 3–709
Adjudication. *See also* central clearance facility
By parent services, 7–101
Central, 6–101
General, 6–100
Of derogatory information, 3–501
Officials, 3–606
Of personnel security clearances, 3–101
Policy, 6–102, 11–101, appendix I
Records, 6–103
Administrative downgrading, 3–405
Administrative inspections, 11–103
Administrative withdrawal, 7–103
Adverse action
Authority for, appendix F
Based on derogatory information, 8–101
Definition, 1–301, 8–100
Exception to policy, 8–202
Final, 8–103
Involuntary separation, 8–201
Notification of, 8–202
Procedures, 8–200, 8–201
Reconsideration of, 8–201
Referral for, 8–101
Reinstatement after, 8–300, 8–301
Suspension, 8–102
Adverse information, 1–304, 2–308, 2–309, 9–102, appendix E. *See also* derogatory information
Adverse suitability information, 1–304, 2–200, appendix E. *See also* security standards
Air Force National Guard, 1–327
Alcohol and Drug Abuse Prevention and Control Program (ADAPCP), 5–106
Allegations, 2–402, 3–501, 3–700, 3–701
American Red Cross, 1–201, 3–401, 3–604, 8–200
Applicant, 1–301
Arms, ammunition, and explosives (AA&E), 3–613
Army–Air Force Exchange Service, 1–201, 3–401
Army Investigative Records Repository, 8–201
Army National Guard(ARNG), 1–201, 1–327, 3–302, 3–401, 5–101, 8–201
Army Reserve, U.S.(USAR), 1–302, 8–201. *See also*individual ready reserve
Assistant Chief of Staff for Intelligence, Air Force, 1–321, 5–101
Assistant Chief of Staff for Intelligence, Army, 1–321, 5–101
Assistant Secretary of Defense (Legislative Affairs), 3–404
Attorneys, 3–404
Automated data processing (ADP)positions, 3–101, 3–614, 3–710, appendix K
Automation security, 3–504
Background investigation (BI)
By the Department of Justice, 3–404
Definition, 1–302
Delay in completion, 3–204
Description, 2–304, appendix B
For critical–sensitive positions, 3–203
Included in SBI, 1–325
Information sources, appendix B
NAC, a part of, 2–301
Table for request, appendix D
Briefing, 9–200–9–204, appendix L
Building passes, DOD, 3–607
Central adjudication facilities, DOD, 6–101
Central Clearance Facility (CCF), U.S. Army
Adjudicates derogatory information, 3–501
Allegations to, 3–501
Authority for debrief from SCI, 3–501
Central adjudication facility for Army, 6–101, 11–101
Clearance determinations made by, 3–504, 8–201
Clearance submitted to, 3–401
Confirms clearances, 3–408, 3–504
Definition, 1–304
Delegates interim clearances, 3–401
Determines LAA, 3–403
Enters determinations in DCSI, 6–103
Forwards determination appeals, 8–201
Grants/denies/revokes clearances, 4–103, 11–101
Investigation waivers submitted to, 3–501
Obtains CIA/FBI/INS checks, 3–501
Proof of citizenship to, 3–501
Reports made by, 11–102
Waiver from instructions, 3–501
Central Intelligence Agency (CIA), 2–305
Central Security Service, 1–321
Chemical agents, 3–610
Chemical Personnel Reliability Program, 3–504
Chemical surety, 1–327
Citizenship. *See also* foreign nationals
Dual, 3–406
Naturalized, 3–402, 3–501
Of U.S. nationals, 1–314
United States, 1–330, 2–100, 3–501
Civilians, DA. *See also*consultants; Office of Personnel Management
Application of program to, 1–201
Clearances for, 3–400
In critical–sensitive positions, 3–203, 3–204
Investigations of, 3–200–3–205
Mobilization of, 3–205
NACIs on, 2–302
PSI of, 1–318
Presidential support by, 3–503
Recorded in DCSI, 1–304
Reinstatement of, 8–300, 8–301
Removal of, 2–402
Retired, 3–205
Service computation, 1–302, 1–327
Summer hires, 1–201, 3–202, 3–401
Classified information, 1–303. *See also* access to classified information; sensitive duty; TOP SECRET
Classified Information Procedures Act (CIPA), 3–404
Clearance. *See* security clearance
Communications security (COMSEC), 3–407
Communist–controlled countries, appendix H, appendixL
Competent medical authority, 1–303
Computer positions, 3–101, 3–614, 3–710, appendix K
Congressional staff, 3–404
Consultants, DA, 1–201, 1–318, 1–327, 3–400, 8–200
Continuing security responsibilities, 9–100 through 9–104
Contract guards, 3–612
Contractors, DA
Application of regulation to, 1–201
PSI of, 1–318
Presidential support by, 3–503
Recorded in DCSI, 1–304
Service computation, 1–302, 1–327
Counterintelligence (CI) agencies, 2–401, 2–403
Credit bureaus, 1–314, 1–317
Criminal conduct, 2–200, 2–402, 8–201, 8–202
Criminal Investigation Command, U.S.Army, 2–402, 3–401
Critical military duties, 3–703
Critical nuclear duty positions, 3–711
Critical–sensitive positions, 3–101, 3–203, 3–204, appendix K
Customs inspectors, 3–603
Defense Central Index of Investigations(DCII)
Checks of, 4–102
DCSI, a subsystem of, 1–304
Definition, 1–303
Determinations entered in, 6–103
Investigations filed in date sequence, 3–401
LAAs recorded in, 3–403
Name checks made with, 3–404
Termination statement information, 9–204
Defense Central Security Index (DCSI), 1–304, 6–103
Defense Criminal Investigative Service (DCIS), 1–303
Defense Industrial Security Clearance Office(DISCO), 3–604, 3–612
Defense Intelligence Agency (DIA), 1–321
Defense Investigative Service (DIS)
BIs/SBIs made by, 3–203

Conduct of SII, 2–306
Congressional staff investigated by, 3–404
Data to DCII, 1–303
NACs/ENTNACs made by, 3–401
Reporting channels, 8–101
Requests for BIs/SBIs to, 3–104
Responsibilities and jurisdiction, 2–400 through 2–404, 5–104, 7–101,
Defense security briefing, appendix L
Department–determined personnel security system(DDPSS), 1–304
Department of Defense (DOD), 1–305, 4–101, 8–101. *See also* DOD heads of Components
Department of Energy, 4–103
Department of Justice(DOJ), 3–404
Deputy Assistant Secretary of the Army for Military Personnel, Equal Opportunity and Human Resources, 11–101
Deputy Chief of Staff for Intelligence (DCSINT)
Clears State officials, 3–404
Determines geographic assignments, 1–326
LAAs reported to, 3–403
Program responsibilities, 11–101
Reports made to, 11–102
Requests for investigation to, 3–615
Standards reviewed by, 6–101
Waives investigations, 3–801
Deputy Chief of Staff for Personnel (DCSPER), 11–101
Deputy Under Secretary of Defense for Policy
Approval of PRs, 3–708
Authority for investigations, 2–400
Clearance for naturalized citizens, 3–402
Investigation priority approval, 5–104
Program information to, 11–101
Scope of SII determined by, 2–306
Special Access investigations approved by, 3–506
Termination statements to, 9–204
Derogatory information. *See also* adverse information; criminal conduct; nonderogatory cases
Adjudicated by CCF, 3–501
As basis for adverse action, 8–101 through 8–103
Definition, 1–304
Minor, 1–311
Revealed during enlistment/appointment, 3–301
Significant, 1–323, 8–102
Suitability, 2–402
Designated countries, 3–402, 3–501, 3–611, 9–103, appendix H
Determinations. *See* personnel security determination
Director of Central Intelligence (DCI), 1–321
Director of Naval Intelligence, 1–321
Disqualification, 3–701
DOD heads of Components
Administer inspections, 11–103
Administer security programs, 11–101
Determine position functions, 7–100
Establish internal controls, 10–101
Evaluate status of personnel, 9–100
Identification of, 1–307
Management responsibilities, 9–101
Periodically brief personnel, 9–200
DOD National Agency Check and written inquiries (DNACI), 1–314, 2–303, 4–103, appendix B, appendix D. *See also* Industrial Security Program, DOD
Dual citizenship, 3–406
Education and orientation personnel, 3–101, 3–611
Employment records, 1–313, 1–314, 1–317
Enlistment, 3–300, 3–301
Entrance investigation, 3–101 through 3–103
Entrance National Agency Check (ENTNAC), 1–306, 2–301, 3–301
Executive branch, 3–404
Extraordinarily sensitive duty, 3–706
Federal Bureau of Investigation (FBI)
Conducts SBIs, 2–305
Counterintelligence activity, 2–401, 2–403
Fingerprints provided to, 5–105
Individual reports to, 9–204
Provides data for NAC, 1–312
Provides data to CCF, 3–501
Provides no data for ENTNAC, 1–306
Federal judiciary, 3–404
Federal Personnel Manual, OPM, 3–201, 8–201
Federal service, 1–302, 3–400, 3–504, 3–602, 3–603, 4–103
Fingerprints, 1–306, 1–312, 5–105, 5–106
Foreign family members, 2–200, 2–308, 3–501
Foreign nationals
Access to classified information, 3–403, appendix F
Employed by the United States overseas, 3–608, 3–707
Employed with OPM approval, 2–100
In nonsensitive positions, 3–201
NACI waived for temporary employees, 3–201
Foreign source information, 3–407, 10–105
Foreign travel briefing, 9–203, appendix L
Freedom of Information, 8–201, 10–105
General Accounting Office (GAO), 1–304
General Counsel, 11–101
General Officer Management Office, 9–204
General Officers, 3–408, 9–204
Governors of U.S. States, 3–404
Guards, 3–612
Hostage situations, 1–318, 2–308, 2–403
Immigrant aliens, 1–308, 1–310, 3–303, 3–403
Immigration and Naturalization Service (INS), DOJ, 3–501
Individual Ready Reserve (IRR), USAR, 1–302, 1–327, 3–304
Induction, 3–300
Industrial Security Program, DOD, 1–302, 1–327, 3–501. *See also* Defense Industrial Security Clearance Office
Information systems, 3–614
Inspections, 11–101, 11–103
Intelligence and Security Command, U.S. Army(USAISC), 8–201
Interim security clearance, 1–309, 3–303, 3–401, 7–101
Investigation of personnel. *See also* Privacy Act; Waiver of Investigation
Authorized to grant access to SCI, 3–605
Authorized to issue clearances, 3–605
Contract guards, 3–612
During mobilization, 3–801
Exceptions to, 3–201, 3–204
Expanded, 2–309
Foreign nationals overseas, 3–608
In education and orientation, 3–611
In information systems, 3–614
In investigative support, 3–609
On clearance and adjudication boards, 3–606
On entry, 3–301 through 3–303
Overseas, 2–404, appendix J
Priorities, 5–104
Requests for, 3–615, appendix D
Special agents, 3–609
Transporters of arms and explosives, 3–613
With access to chemical agents, 3–610
With access to classified information, 3–708
With DOD building passes, 3–607
Investigative agencies, 2–400
Investigative data collection, 2–502
Investigative records
Access restrictions, 10–102
Destruction, 10–104
Disposition, 10–104
In date sequence in DCII, 3–401
Non–DOD, 4–102
Repositories, 8–201, 10–104
Request for, 8–201
Safeguarding, 10–100 through 10–105
Investigative requirements
Exceptions to, 3–201, 3–204, 3–401
For security clearance, 3–401
For Special Access Programs, 3–500 through 3–506
General, 3–100 through 3–104
Waivers of, 3–305
Investigative scope, 2–306, appendix B
Investigative support personnel, 3–609
Investigators, 2–501, 2–504
Joint Chiefs of Staff (JCS), 1–305, 1–307, 5–101
Judge Advocate General, Office of The (OTJAG), 3–404, 8–201
Letter of intent(LOI), 6–101, 8–201
Limited access authorization (LAA)
Authority to grant, appendix F
Conditions for grant, 3–403
Definition, 1–310
Determined by CCF, 3–403
Grantees subject to PRs, 3–707
Procedures for, appendix J
Reasons for grant, 2–100
Reported to DCSINT, 3–403
Local agency check (LAC), 1–317, 2–304, appendix B
Major Army command (MACOM), 1–310, 3–305, 3–601, 11–102
Medical authority, 1–303, 2–504, 5–106, 5–107
Medical evaluation of personnel
By medical authorities, 1–303, 2–504, 3–504, 5–106, 5–107,
Refusal to submit to, 2–200
Reports of, 5–106
Medical personnel, 3–303, 3–503
Medical records
Checks of, 2–502

Collection of, 2–504
Evaluation of, 2–504
Favorable review for TOP SECRET, 3–401
Investigative information from, 5–106
Members of Congress, 3–404
Merit Systems Protection Board, 8–101
Military academies, 1–327
Military appointment, 3–300, 3–301, 3–303
Military duties, 3–703
Military Personnel Records Jacket, 3–801, 7–101, 8–201
Military Reserve Force, 1–327
Military retirees, 3–304
Military Service standard, 2–102
Military Traffic Management Command(MTMC), 3–613
Minor derogatory information, 1–311
Mobilization
DA–directed, 3–801
Exercises, 3–305
Investigations, 3–305
Of DOD civilian retirees, 3–205
Of military retirees, 3–304
Name checks, 3–404
National Agency Check (NAC). *See also* entrance NAC
Definition, 1–312, 2–301
Included in BI/SBI, 2–301, 2–304
Included in PR, 1–317, 2–301
Table for request, appendix D
National Agency Check and written inquiries (NACI). *See also* DOD NAC and written inquiries
Conducted by OPM, 1–313, 2–302, 3–201, 4–103
Definition, 1–313
Table for request, appendix D
Waived for foreign temporaries, 3–201
National Archives, 10–104
National of the United States, 1–314
National security, 1–315
National Security Agency (NSA), 1–201, 1–303, 1–321
Need to know, 1–316, 1–324
Nonappropriated Fund employees, 3–602, appendix F
Noncritical–sensitive positions, 3–101, 3–202, 3–204, appendix K
Nonderogatory cases, appendix E. *See also* derogatory information
Nonsensitive positions, 3–101, 3–201, appendix K
North Atlantic Treaty Organization (NATO), 3–407, 3–505, 3–705, 7–102
Nuclear duty positions, 3–504, 3–711, appendix F
Nuclear Regulatory Commission, 4–103
Nuclear surety, 1–327
Nuclear Weapon Personnel Reliability Program (PRP), 3–504
Office of Personnel Management (OPM)
Approves foreign national employment, 2–100, 3–201
Conducts NACIs, 1–313, 2–302, 3–201
Conducts SBIs, 2–305
Federal Personnel Manual, 3–201, 8–201
Removal of Federal employees, 2–402
Office of the Secretary of Defense (OSD), 1–305, 1–307. *See also* Washington Headquarters Services
Official personnel folder (OPF), 3–204, 7–101, 8–201
One–time access, 3–407, 3–501
Periodic reinvestigation (PR)
Authority for, 3–700, 3–708, appendix F
Definition, 1–317
Includes NAC, 1–317, 2–301
Requirement for, 2–307, 3–700 through 3–710
Scope, appendix B
Personal interviews, 2–308, 2–503, appendix G
Personal security questionnaire (PSQ), 2–200, 3–202
Personnel security, 1–317
Personnel Security and Surety Program, 3–301
Personnel security clearance. *See* security clearance
Personnel security determination
Acceptance, 4–100 through 4–102
Access to, 10–102
Authority, 2–500, appendix F
By DOD, 4–102
Entered in DCII, 6–103
For nuclear duty positions, 3–504
Unfavorable, 1–329
Personnel security investigation (PSI). *See also* waiver of investigation
Additional information, 5–106
Authority for, 2–400
Authorized requestors, 2–500, 5–101
Criteria for requests, 5–102
Definition, 1–318
DOD, 4–101
Evaluation of information, 6–102
Limitations of, 2–500 through 2–505
Overseas, 2–404
Personal data provided, 5–105
Prior, 4–100, 4–101
Priority requests, 5–104
Request procedures, 5–103, appendix C
Requests for, 5–100
Scope, 1–319, 2–300
Subject of, 5–105
Types of, 2–300 through 2–309
Personnel security record, 8–300
Polygraph examination, 1–318, 2–505, 3–403
Positions, 3–101–3–103
Prenomination interviews, appendix G
Presidential support activities, 3–503, 3–704, appendix F
Privacy Act
Confidentiality provisions, 8–201
Foreign information protected by, 10–105
Information direct from subject, 5–105
Makes personal interview necessary, 2–308
Notification of interview purpose, 2–503
Request for files under, 8–201
Restrictions on investigators, 2–504
Statement furnished, 5–105
Program management, 11–100 through 11–103
Reciprocal acceptance of determinations and clearances, 4–100 through 4–103
Red Cross, 1–201, 3–401, 3–604, 8–200
Reinstatement, 8–300, 8–301
Reinvestigation, 3–700. *See also* periodic reinvestigation
Request procedures
For BI/SBI, appendix D
For DIS BI/SBI, 3–104
For grant of LAA, appendix J
For NAC/NACI, appendix D
For PSI, 2–500, 5–100 through 5–104, appendix C
Reserve Components (RC), 3–302, 3–303, 8–201
Reserve Officers' Training Corps (ROTC), 1–302, 1–327, 3–301
Restricted areas, 3–601
Restricted data, appendix F
Retired personnel, 3–205, 3–304, 3–408
Revocation of security clearance, 1–318, 3–400
Screening systems, 2–308
Secret Service, 2–305
Security briefing, appendix L
Security clearance. *See also*Defense Central Security Index; Central clearance facility; Personnel security determination
Adjudication of, 3–101
Authority to grant, 3–400, appendix F
By commanders, 3–401
By the Department of Justice, 3–404
Definition, 1–320
Denial of, 1–304, 3–400, 6–101, 7–100, 7–101
For chemical duty, 3–504
For nuclear duty, 3–504
Interim, 1–309, 3–303, 3–401, 7–101
Investigative requirements, 3–401, 3–501
Issuance, 3–405, 7–100, 7–101
Of naturalized aliens, 3–402
Reciprocal acceptance of, 4–103
Requirements, 1–201
Restrictions on issuance, 3–405
Revocation, 1–318, 3–400, 6–101, 7–100, 7–101
Waivers of criteria, 3–501
Withdrawal of, 7–103
Security designation of positions, 3–100 through 3–103
Security eligibility, 9–100
Security standards. *See also*adverse suitability information; suitability information
Application, 2–100
Clearance, 2–101
Criteria for, 2–200, 3–101, appendix E
For sensitive positions, 2–101
Military service, 2–102
Review of, 6–101
Senior Executive Service (SES), 3–407
Senior Officer of the Intelligence Community(SOIC), 1–321
Sensitive compartmented information (SCI)
Access to, 3–407, 3–501, 3–702
Authority to grant access to, appendix F
Definition, 1–321
General, 3–501
Protection of, 8–101
Revocation of access to, 1–329
Sensitive duty. *See* sensitive positions
Sensitive positions
Assignment to, 2–100
Authority to designate, 3–102, appendix F
Automated data processing, 3–101, appendix K
Billet control system, 3–104

Civilians in, 3–200 through 3–205
Criteria for designation, 3–101
Critical–sensitive, 3–101, 3–203, 3–204
Definition, 1–322
Designation of, 3–100
Extraordinarily sensitive, 3–706
Limitation of, 3–103
Noncritical–sensitive, 3–101, 3–202, 3–204
Security designation of, 3–101, 3–102
Standards for, 2–101
Very sensitive, 3–708
Separation, 8–201
Service, 1–327
Sexual misconduct, 2–200, appendix I
Significant derogatory information, 1–323, 8–102
Single Integrated Operation Plan—extremely sensitiveinformation (SIOP–ESI), 3–502, 7–102, appendix F
Special Access Programs
As criterion for critical military duty, 3–703
As criterion for sensitive position, 3–101
Definition, 1–324
Investigative requirements, 3–500 through 3–506
Revocation of access to, 1–329
Special agents, 3–609
Special background investigation (SBI)
Conducted by DIS, 3–203
Conducted by FBI, 2–305
Conducted by OPM, 2–305
Definition, 1–325
Investigative requirements, appendix B
NAC included in, 2–301, 2–304
Partial completions, 3–204
Request procedures, appendix D
Requested from DIS, 3–104
Required for SIPO–ESI access, 3–502
Special investigative inquiry (SII), 1–326, 2–306, 2–402, 3–701
Specific geographic area, 1–326
Staff security officer (SSO), 2–308, 3–501, 8–101, 8–102
State government, 3–404
Subversive affiliations, 2–401, 3–501
Subversive organizations, 1–318
Suitability Evaluation Board, DA(DASEB), 8–201
Suitability information, 2–402. *See also* adverse suitability information; security standards
Supreme Court of the United States, 3–404
Suspension of access, 1–327, 8–101, 8–102
Termination, 8–103, 8–300, 9–204
TOP SECRET
Access requires PR, 3–703, 3–709
Access to, 3–101, 3–104, 3–401
Authority to grant access, appendix F
Billet control system, 3–104, 3–401
Criteria for military access, 3–703
Criterion for critical–sensitive position, 3–101
Interim clearance, 3–401
Investigative requirements, 3–401
Total Army Personnel Agency (TAPA), 1–326, 8–201
Transportation of arms, 3–613
Troop Program Units, USAR, 1–302
Unfavorable administrative action, 1–328. *See also*adverse action
Unfavorable investigations, 6–101
Unfavorable personnel securitydetermination, 1–329
Unit authorization documents (MTOE/TDA), 3–104
United Service Organizations (USO), 1–201, 3–401, 3–604, 8–200
U.S. citizen, 1–330, 2–100, 3–501
Very sensitive positions, 3–708
Waiver of foreign connections, 3–501
Waiver of investigation
Authority for, 3–800
During mobilization, 3–801
For temporary employees, 3–201
In combat, 3–801
Requirements, 3–305, 3–800, 3–801
submitted to CCF, 3–501
Washington Headquarters Services (WHS), OSD, 3–404, 5–101
White House Military Office, 3–503
Withdrawal ofclearance, 7–103

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.63

PIN:	064502–000
DATE:	08-18-99
TIME:	10:15:28
PAGES SET:	67

DATA FILE:	r380.fil
DOCUMENT:	AR 380–67
DOC STATUS:	NEW PUBLICATION