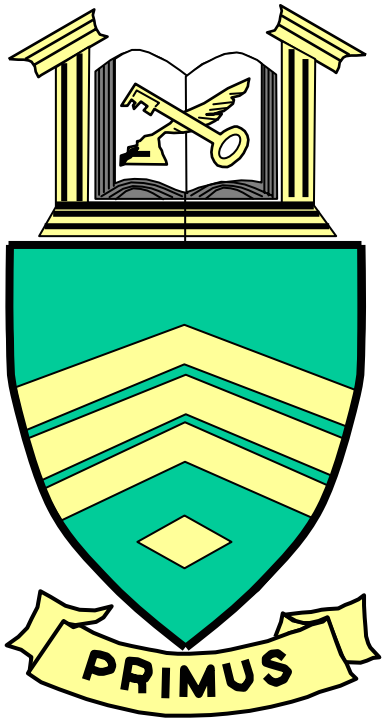
U.S. ARMY SERGEANTS MAJOR ACADEMY (FSC-TATS)

R653 JUN 06

ENFORCE PERSONNEL SECURITY POLICIES

PRERESIDENT TRAINING SUPPORT PACKAGE



THIS PAGE LEFT BLANK INTENTIONALLY

PRERESIDENT TRAINING SUPPORT PACKAGE (TSP)

TSP Number / Title	R653 / ENFORCE PERSONNEL SECURITY POLICIES
Effective Date	01 Jun 2006
Supersedes TSP(s) / Lesson(s)	R653, Enforce Personnel Security Policies, Jun 05.
TSP Users	521-SQIM (DL), First Sergeant Course
Proponent	The proponent for this document is the Sergeants Major Academy.
Improvement Comments	Users are invited to send comments and suggested improvements on DA Form 2028, *Recommended Changes to Publications and Blank Forms.* Completed forms, or equivalent response, will be mailed or attached to electronic e-mail and transmitted to: COMDT USASMA ATTN ATSS DCF BLDG 11291 BIGGS FIELD FORT BLISS TX 79918-8002 Telephone (Comm) (915) 568-8875 Telephone (DSN) 978-8875 E-mail: atss-dcd@bliss.army.mil
Security Clearance / Access	Unclassified
Foreign Disclosure Restrictions	FD5. This product/publication has been reviewed by the product developers in coordination with the USASMA foreign disclosure authority. This product is releasable to students from all requesting foreign countries without restrictions.

PREFACE

Purpose

This Training Support Package provides the student with a standardized lesson plan of instruction for:

Task Number	**Task Title**
Individual	
301-371-1051	Enforce a Personnel Security Program

This TSP Contains

TABLE OF CONTENTS

THIS PAGE LEFT BLANK INTENTIONALLY

ENFORCE PERSONNEL SECURITY POLICIES
R653 / Version 1
01 Jun 2006

SECTION I. ADMINISTRATIVE DATA

All Courses Including This Lesson

Course Number	Version	Course Title
521-SQIM	1	First Sergeant Course

Task(s) Taught(*) or Supported

Task Number	Task Title
INDIVIDUAL	
301-371-1051 (*)	Enforce a Personnel Security Program

Reinforced Task(s)

Task Number	Task Title
704-002-0001	Identify Leader Actions and Tools that Support the Army Management Control Process

Academic Hours

The academic hours required to teach this lesson are as follows:

	Resident Hours/Methods
	35 mins / Study Assignment
	15 mins / Practical Exercise (Performance)
Test	0 hrs
Test Review	0 hrs
Total Hours:	1 hr

Test Lesson Number

	Hours	Lesson No.
Testing (to include test review)	3hrs	E516 version 1

Prerequisite Lesson(s)

Lesson Number	Lesson Title
None	

Clearance Access

Security Level: Unclassified
Requirements: There are no clearance or access requirements for the lesson.

Foreign Disclosure Restrictions

FD5. This product/publication has been reviewed by the product developers in coordination with the USASMA foreign disclosure authority. This product is releasable to students from all requesting foreign countries without restrictions.

References

Number	Title	Date	Additional Information
AR 380-67	PERSONNEL SECURITY PROGRAM	09 Sep 1988	

Student Study Assignments

All material included in this Training Support Package (TSP).

Instructor Requirements

None

Additional Support Personnel Requirements

Name	Stu Ratio	Qty	Man Hours
MSG, FSC graduate, ITC, and SGITC graduate, (Enlisted)	1:14	1	1 hr

Equipment Required for Instruction

Id Name	Stu Ratio	Instr Ratio	Spt	Qty	Exp
None					

* Before Id indicates a TADSS

Materials Required

Instructor Materials:

None

Student Materials:

- TSP.
- Pen or pencil and paper.

Classroom, Training Area, and Range Requirements

None

Ammunition Requirements

Id	Name	Exp	Stu Ratio	Instr Ratio	Spt Qty
None					

Instructional Guidance

None

Proponent Lesson Plan Approvals

Name	Rank	Position	Date
Santa Barbara, Robert A.	GS-09	Training Specialist	
Smith, Sandra	SGM	Chief Instructor, FSC	
Graham, Kevin L.	MSG	Chief, FSC	
Collins, Curtis R.	SGM	Chief, SMC	
Lemon, Marion	SGM	Chief, CMDD	

SECTION II. INTRODUCTION

Method of Instruction: Study Assignment
Technique of Delivery: Individualized, self-paced instruction
Instructor to Student Ratio is: 1:14
Time of Instruction: 5 mins
Media: None

Motivator

Personnel security at the unit level can be the first line of defense against security breaches that may effect the national security. During this lesson you will learn how to enforce personnel security policies within a unit.

Terminal Learning Objective

At the completion of this lesson, you [the student] will:

Action:	Identify requirements for enforcement of a unit personnel security program.
Conditions:	As a first sergeant, in a self-study environment, given AR 380-67.
Standards:	Identified requirements for enforcement of a unit personnel security program IAW AR 380-67.

Safety Requirements

None

Risk Assessment Level

Low

Environmental Considerations

NOTE: It is the responsibility of all Soldiers and DA civilians to protect the environment from damage.

None

Evaluation

At the end of your phase I training and before entering phase II, you will take an on-line, multiple choice examination. It will test your comprehension of the learning objectives from this and other lessons in phase I. You must correctly answer 70 percent or more of the questions on the examination to receive a GO. Failure to achieve a GO on the examination will result in a retest. Failure on the retest could result in your dismissal from the course.

Instructional Lead-In

None

THIS PAGE LEFT BLANK INTENTIONALLY

SECTION III. PRESENTATION

A. ENABLING LEARNING OBJECTIVE

ACTION:	Identify the criteria for access to security information and granting of a security clearance.
CONDITIONS:	As a first sergeant, in a self-study environment, given AR 380-67.
STANDARDS:	Identified the criteria for access to security information and granting of a security clearance IAW AR 380-67.

1. Learning Step / Activity 1. Identify the Criteria for Access to Security Information and Granting of a Security Clearance

Method of Instruction: Study Assignment
Technique of delivery: Individualized, self-paced instruction
Instructor to Student Ratio: 1:14
Time of Instruction: 15 mins
Media: SH-1

To complete this learning step activity, you are to--

- Read the above ELO.
- Read SH-1.

2. Learning Step / Activity 2. Identify the Criteria for Access to Security Information and Granting of a Security Clearance

Method of Instruction: Practical Exercise (Performance)
Technique of Delivery: Individualized, self-paced instruction
Instructor to Student Ratio: 1:14
Time of Instruction: 5 mins
Media: SH-1

Try to complete the questions in this practical exercise without referring to the student handout. Write your answer in the space provided.

- This is a self-graded exercise.
- It should take you approximately 5 minutes to complete the questions.
- Complete questions 1 of PE-1, p C-2.
- Compare your responses with the solutions on p C-4.
- If your response does not agree, review the appropriate reference/lesson material.

CHECK ON LEARNING: The practical exercise serves as a check on learning for ELO A.

B. ENABLING LEARNING OBJECTIVE

ACTION:	Identify the criteria for suspending/revoking access.
CONDITIONS:	As a first sergeant, in a self-study environment, given AR 380-67.
STANDARDS:	Identified the criteria for suspending/revoking access IAW AR 380-67.

1. Learning Step / Activity 1. Identify the Criteria for Suspending/Revoking Access

Method of Instruction: Study Assignment
Technique of delivery: Individualized, self-paced instruction
Instructor to Student Ratio: 1:14
Time of Instruction: 10 mins
Media: SH-1

To complete this learning step activity, you are to--

- Read the above ELO.
- Read SH-1.

2. Learning Step / Activity 2. Identify the Criteria for Suspending/Revoking Access

Method of Instruction: Practical Exercise (Performance)
Technique of Delivery: Individualized, self-paced instruction
Instructor to Student Ratio: 1:14
Time of Instruction: 10 mins
Media: SH-1

Try to complete the questions in this practical exercise without referring to the student handout. Write your answer in the space provided.

- This is a self-graded exercise.
- It should take you approximately 5 minutes to complete the questions.
- Complete questions 2 thru 4 of PE-1, pp C-2 and C-3.
- Compare your responses with the solutions on p C-4.
- If your response does not agree, review the appropriate reference/lesson material.

CHECK ON LEARNING: The practical exercise serves as a check on learning for ELO B.

SECTION IV. SUMMARY

Method of Instruction: Study Assignment
Technique of Delivery: Individualized, self-paced Instruction
Instructor to Student Ratio is: 1:14
Time of Instruction: 5 mins
Media: None

Check on Learning

PE-1 is the check on learning for this lesson.

Review / Summarize Lesson

To assist the commander you need to continue to review the procedures and processes in administering to the personnel security program within your unit. Ensuring a viable program will require your direct supervision.

THIS PAGE LEFT BLANK INTENTIONALLY

SECTION V. STUDENT EVALUATION

Testing Requirements	At the end of your phase I training and before entering phase II, you will take an on-line, multiple choice examination. It will test your comprehension of the learning objectives from this and other lessons in phase I. You must correctly answer 70 percent or more of the questions on the examination to receive a GO. Failure to achieve a GO on the examination will result in a retest. Failure on the retest could result in your dismissal from the course.
Feedback Requirements	**NOTE:** Feedback is essential to effective learning.

THIS PAGE LEFT BLANK INTENTIONALLY

STUDENT QUESTIONNAIRE R653

Directions

- Enter your name, your rank, and the date you complete this questionnaire.

Rank:_____ Name: _____ Date: _____

- Answer items 1 through 6 below in the space provided.
- Fold the questionnaire so the address for USASMA is visible.
- Print your return address, add postage, and mail.

Note: Your response to this questionnaire will assist USASMA in refining and improving this course. While completing the questionnaire, answer each question frankly. Your assistance helps build and maintain the best curriculum possible.

Item 1	Do you believe you have met the learning objectives of this lesson?
Item 2	Was the material covered in this lesson new to you?
Item 3	Which parts of the lesson were most helpful to you in learning the objectives?
Item 4	How could we improve the format of this lesson?
Item 5	How could we improve the content of this lesson?
Item 6	Do you have additional questions or comments? If you do, please list them here. You may add additional pages if necessary.

_____
_____
_____

ATTN ATSS DCF
COMDT USASMA
BLDG 11291 BIGGS FLD
FORT BLISS TX 79918

----------(Fold Here)----------

Appendix A - Viewgraph Masters (N/A)

Appendix B - Test(s) and Test Solution(s) (N/A)

PRACTICAL EXERCISE 1

Title

ENFORCE PERSONNEL SECURITY POLICIES

Lesson Number / Title

R653 version 1 / ENFORCE PERSONNEL SECURITY POLICIES

Introduction

None

Motivator

Personnel security at the unit level can be the first line of defense against security breaches that may effect the national security. During this lesson you will learn how to enforce personnel security policies within a unit.

Terminal Learning Objective

At the completion of this lesson, you [the student] will:

ACTION:	Identify requirements for enforcement of a unit personnel security program.
CONDITIONS:	As a first sergeant, in a self-study environment, given AR 380-67.
STANDARDS:	Identified requirements for enforcement of a unit personnel security program IAW AR 380-67.

Safety Requirements

None

Risk Assessment

Low

Environmental Considerations

None

Evaluation

At the end of your phase I training and before entering phase II, you will take an on-line, multiple choice examination. It will test your comprehension of the learning objectives from this and other lessons in phase I. You must correctly answer 70 percent or more of the questions on the examination to receive a GO. Failure to achieve a GO on the examination will result in a retest. Failure on the retest could result in your dismissal from the course.

Instructional Lead-In

None

Resource Requirements

Instructor Materials:

None

Student Materials:

- TSP.
- Pen or pencil and paper.

Special Instructions

None

THIS PAGE LEFT BLANK INTENTIONALLY

Procedures

This is a self-graded exercise. Circle the letter, fill-in the blank, or write in your answer on the following questions. Upon completion, compare your responses to the correct responses in the Solution for Practical Exercise 1, p C-4.

Question 1 What is the exact criteria for entitlement to knowledge of, possession of, or access to classified defense information?

a. Solely by virtue of office, position, grade, rank, and the need to know.

b. Position, grade, and compelling national security reasons.

c. Official military duties require such access, and the appropriate security clearance has been granted.

d. Proper degree of security clearance and meet the access parameters within the organization.

Question 2 Commanders must report credible derogatory information to the Commander, Central Clearance Facility on what category of personnel?

a. For all personnel who hold Top Secret clearances.

b. Only if the commander believes the information received is serious.

c. For all personnel regardless of the type/level of clearance held.

d. For all personnel regardless of whether or not they hold any type of clearance.

Question 3 Upon receipt of a Letter of Intent (LOI) from CCF to deny or revoke access, the individuals can do which of the following?

a. Respond with an explanation or rebuttal to the LOI.

b. Have the commander decide on action to revoke or suspend access not to exceed 60 days or upon adjudication of the individual's rebuttal, whichever comes first.

c. Voluntarily request suspension of access to classified material until successful resolution of the denial or revocation action.

d. Appeal to their commander to have the derogatory information removed from their Official Personnel Military File (OMPF).

Question 4 With regards to allegations related to disqualification, what type of process would be appropriate on an individual who develops questionable behavior patterns?

a. The unit should initiate a periodic reinvestigation (PR) to ascertain the facts.

b. The unit should request a special investigative inquiry (SII) to resolve issues in doubt.

c. The higher headquarters Security Manager should submit a DD Form 398-2.

d. The unit should request an updated National Agency Check (NAC) and Local Area

Feedback Requirements None

SOLUTION FOR
PRACTICAL EXERCISE 1

Question 1 The correct response is:

c. official military duties require such access, and the appropriate security clearance has been granted.

Ref: AR 380-67, paragraph 2-100b and paragraph 7-102 (ELO A)

Question 2 The correct response is:

d. For all personnel regardless of whether or not they hold any type of clearance.

Ref: AR 380-67, paragraph 8-101b(4) (ELO B)

Question 3 The correct response is:

a. Respond with an explanation or rebuttal to the LOI.

Ref: AR 380-67, paragraph 8-201a(2), b, and c (ELO B)

Question 4 The correct response is:

b. The unit should request a special investigative inquiry (SII) to resolve issues in doubt.

Ref: AR 380-67, paragraph 3-701 (ELO B)

THIS PAGE LEFT BLANK INTENTIONALLY

Appendix D

HANDOUTS FOR LESSON: R653 version 1

This appendix contains the items listed in this table---

Title/Synopsis	Pages
SH-1, Extracted material from AR 380-67	SH-2-1

THIS PAGE LEFT BLANK INTENTIONALLY

Student Handout 1

Extracted Material from AR 380-67

This student handout contains 18 pages of extracted material from the following publication:

AR 380-67, Personnel Security Program, 9 Sep 1988

Chapter 1	pages 1 thru 5
Chapter 2	pages 5 and 6
Chapter 3	pages 11 and 19
Chapter 5	pages 22 and 23
Chapter 6	pages 23 and 24
Chapter 7	pages 24 and 25
Chapter 8	pages 25 thru 28
Chapter 9	pages 28 thru 30
Chapter 10	page 30
Appendix H	page 45

Disclaimer: The training developer downloaded the extracted material from the United States Army Publishing Agency Home Page. The text may contain passive voice, misspellings, grammatical errors, etc., and may not be in compliance with the Army Writing Style Program.

THIS PAGE LEFT BLANK INTENTIONALLY

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

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

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.

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

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