



# U.S. ARMY ARMOR CENTER AND FORT KNOX



## PERSONNEL SECURITY PROGRAM

Prepared by

Security Division  
G3/Directorate of Plans,  
Training, and Mobilization  
Fort Knox, Kentucky 40121-5000

**HOME OF MOUNTED WARFARE**

Headquarters  
U.S. Army Armor Center and Fort Knox  
Fort Knox, Kentucky 40121-5000  
12 February 1998

C1, USAARMC Pam 380-67

USAARMC Pamphlet 380-67

Change 1

## Security

### PERSONNEL SECURITY PROGRAM

Summary. This change incorporates revisions to USAARMC Pamphlet 380-67 that establish procedures for processing security actions.

Suggested improvements. The proponent of this pamphlet is the Security Division, G3/Directorate of Plans, Training and Mobilization. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, USAARMC and Fort Knox, ATTN: ATZK-PTF-P, Fort Knox, Kentucky 40121-5000.

Supersession notice. This change supersedes all previous Interim Changes, and Personnel Security Update memorandums prior to September 1997. Change 1 has been incorporated in the USAARMC Pamphlet 380-67. The USAARMC Pamphlet 380-67 with changes is available at G3/DPTM, Security Office. To obtain a copy of the updated Pamphlet bring a pre-formatted diskette to G3/DPTM, Security Office.

1. USAARMC Pamphlet 380-67, 21 October 1994, is changed as follows:

✓ Page 1-1, paragraph 1-I. Delete the words "Federal Personnel Manual Supplement 296-33, 30 April 1981," change to read: Office of Personnel Management, June 1994.

✓ Page 2-4, paragraph 2-4a. In the first sentence after the word "years" add a period and delete the rest of the sentence.

✓ Page 2-5, paragraph 2-6b. In the first sentence after the word "SC5" delete (194th Armored Brigade report).

- ✓ Page 3-~~2~~<sup>1</sup>, paragraph 3-5. After the second sentence add the following: Cancellation can also be accomplished by telephoning the security office and supplying them the name and reason for cancellation. The security office will then cancel the open investigation.
- ✓ Page 3-~~4~~<sup>3</sup>, paragraph 3-7c. After the third sentence, insert the following sentences: Include your office in the "from" block. SUBJECT's name, rank and social security number must be legible and complete. Include unit address and the security manager's telephone number.
- ✓ Page 3-4, paragraph 3-8. In the second sentence, remove "(DD Form 398-2 or DD Form 1879)" replace it with: investigative forms.
- ✓ Page 3-5, paragraph 3-8b. Delete this paragraph.
- ✓ Page 3-6, paragraph 3-10f. In the second sentence delete the word "and" after the word Islands and add the words: and the "Republic of Palau".
- ✓ Page 4-1, paragraph 4-3. In the last sentence after the word "The" change "Chief Personnel Security Branch" to read: CDR/Director of your activity.
- ✓ Page 4-2, paragraph 4-3. In the fourth sentence after the word "without" delete the rest of the sentence, change to read: approval by the CDR/Director of your activity.
- ✓ Page 4-2, paragraph 4-3. Add the following at the end of the fifth sentence: by the CDR/Director of your activity.
- ✓ Page 4-2, paragraph 4-4a. In the second sentence change the word "submitted" to read: prepared.
- ✓ Page 4-2, paragraph 4-4b. In the first sentence after the word "approved, delete the rest of the sentence, change to read: assign a control number to the SF 52-B.
- ✓ Page 4-2, paragraph 4-4b. After the last sentence add the following sentence: Furnish Security Division a copy of the approved SF 52-B.

- ✓ Page 4-2, paragraph 4-5. In the first sentence change the word "record" to read: roster. In the same sentence after the word "be" add the following: prepared and.
- ✓ Page 4-2, paragraph 4-5. Delete the second, third, fourth and fifth sentence, add the following: Prepare the roster bi-yearly (Jan & Jul). Furnish a copy of the roster to the Personnel Security Branch and CPAC. If major changes occur to the roster prior to the preparation of the bi-annual report, prepare a corrected roster and furnish the Personnel Security Branch along with CPAC a copy of the correct roster.
- ✓ Page 4-4, paragraph 4-8c(2). In the second sentence after the acronym "SSBI" add the following: or previous valid NACI, NAC, or ENTNAC.
- ✓ Page 4-6, paragraph 4-10. Delete this paragraph.
- ✓ Page 4-6, paragraph 4-11. Change to read: 4-10.
- ✓ Page 4-6, paragraph 4-12. Change to read: 4-11.
- ✓ Page 5-1, paragraph 5-1. Delete the last sentence in this paragraph. Add the following sentence: The Electronic Personnel Security Questionnaire (EPSQ) forms are the only investigative forms the Personnel Security Branch will accept with the exception to paragraph 5-6(b).
- ✓ Page 5-2, paragraph 5-4a. Change "DD Form 398-2 (National Agency Questionnaire (NAQ))- revised Mar 90 (or any future version)" to read: National Agency Check Security Information (Security Officers EPSQ version) and an SF 86 (Security Clearance Application) (SUBJECT's version of the EPSQ).
- ✓ Page 5-2, paragraph 5-5a. In the first sentence delete everything up to the word "original", replace the first part of the sentence with the following: National Agency Check Security Information along with an SF 86 (Security Clearance Application).
- ✓ Page 5-2, paragraph 5-6. In the fourth sentence add the following after the word "(SBI)": or Single Scope Background Investigation (SSBI).

✓ Page 5-2, paragraph 5-6b. Delete the words "Sensitive Positions" change to read: National Security Position.

✓ Page 5-2, paragraph 5-6d. Add the following after the word "appointment": If the SF 171 is not used, the following must be submitted: Resume or OF 612 (Optional Application For Federal Employment) along with the OF 306 (Declaration For Federal Employment).

✓ Page 5-3, paragraph 5-8a. Delete "revised March 1990 (or any future revision)", change to read: (EPSQ version only).

✓ Page 5-3, paragraph 5-8b. Delete the following: DD Form 398 (Personnel Security Questionnaire (PSQ)- revised March 1990 (or any future revision), change to read: SF 86 (Security Clearance Application (EPSQ Version only) Items 4-6 must cover the last 10 years. The EPSQ 2.1c version will not let you enter information prior to 7 years, therefore, the remaining 3 years should be entered into the remarks section of Item 5, 6 and 7 or in the Remarks Section Item 43.

✓ Page 5-2, paragraph 5-8c. Delete this paragraph.

✓ Page 5-3, paragraph 5-8d. Change to read: 5-8c.

✓ Page 5-3, paragraph 5-8e. Delete everything after the word "access," change to read: A statement from the commander explaining foreign affiliation with non-U.S. citizens or relatives. This includes the proposed date of marriage on individuals intending to marry a foreign national.

✓ Page 5-4, paragraph 5-10a(1). In the second sentence delete the number "5" and insert the number "7". In the same sentence delete the words "DD Form 398 will be completed to," change to read: SF 86, Items 4, 5, and 6 will.

✓ Page 5-4, paragraph 5-10a(3). Delete this subparagraph.

✓ Page 5-4, paragraph 5-10b. At the end of the sentence delete the word "of", change to read: that fingerprints charts are not required. Delete the subparagraphs (1) and (2).

✓ Page 5-5, paragraph 5-11. Delete the paragraph. Paragraph 5-11 is superseded as follows: SECRET-PR must be submitted at the

15th year anniversary date. If the SECRET-PR is not submitted within 30 days the 15 year anniversary date, access must be downgraded to CONFIDENTIAL.

✓ Page 5-5, paragraph 5-11a. Delete this paragraph. Paragraph 5-11a is superseded as follows: A SECRET-PR consist of the following forms: Original SF 86 and original National Agency Check Security Information from plus five single sided copies of each form.

✓ Page 5-5, paragraph 5-11b. Delete this paragraph. Paragraph 5-11b is superseded as follows: If the investigation on military personnel is over 17 years an original NAC must be submitted. This is no longer considered a Secret-PR.

✓ Page 5-5, paragraph 5-12. Delete this paragraph. Paragraph 5-12 is superseded as follows: Security clearances will be downgraded on all individuals who are not currently requiring access nor hold a military specialty requiring a security clearance, and who investigations is outdated. Downgrading is accomplished by submitting an original DA Form 5247-R, along with the original DA Form 873, plus a copy of each form.

✓ Page 5-5, paragraph 5-12(a). Delete this paragraph. Paragraph 5-12(a) is superseded as follows: The name, grade and SSN blocks of the DA Form 873 must be verified to attest to the accuracy of the data. Needed correction(s) may be "pen and inked" on the form and indicated in the Remarks section of the DA Form 5247-R.

✓ Page 5-5, paragraph 5-12(b). Delete this paragraph. Paragraph 5-12(b) is superseded as follows: The individual's status of federal service must be verified and the year, month and day (YYMMDD) of continuous Federal service without a break exceeding 24 months must be indicated. The remarks section must also include the nature of the request (e.g., Downgrade clearance to...).

✓ Page 5-6, paragraph 5-17. In the last sentence delete " 18, DD Form 398," change to read: 12, DD Form 1879.

✓ Page 6-1, paragraph 6-2. In the first sentence delete the "has", change to read: for civilians have. After the word "Roster" delete the rest of the sentence.

- ✓ Page 6-2, paragraph 6-4. In the second sentence delete "DD Form 398-2," change to read: National Agency Check Security Information (Security officer version of the EPSQ).
- ✓ Page 6-2, paragraph 6-4b. Insert the following subparagraphs: (1) A NACI conducted on civilian employees based on an SF 85 is insufficient for determining security clearance eligibility. Civilian employees being nominated for a CONFIDENTIAL or SECRET security clearance based on an SF 85 NACI must complete an SF 86 (EPSQ version) complete items 1-3 and 17-40. The security manager will review the form and if no potentially adverse information is identified the completed SF 86 will be added as an enclosure to the DA Form 5247-R. If adverse information is revealed on the SF 86, SUBJECT must complete the SF 86 in its entirety prior to it being attached to the DA Form 5247-R.  

(2) Proof of the investigation will be attached to the DA Form 5247-R along with the SF 86.
- ✓ Page 6-2, paragraph 6-5. Change as follows: (1) Add subparagraph 6-5a. Subparagraph 6-5a should begin with the first word "Request" in the second sentence and end with the last word in the third sentence "records."  

(2) Add subparagraph 6-5b. All requests for interim security clearance must be submitted via DA Form 5247-R. If your are submitting an investigation and interim security clearance is required, DA Form 5247-R is also required.
- ✓ Page 6-3, paragraph 6-6b(2). In the first sentence after "873" delete the phrase: and a copy of the SIDPERS form. In the second sentence after the word "alone" delete the phase: or SIDPERS documents alone.
- ✓ Page 6-4, paragraph 6-7b(5). Delete this paragraph.
- ✓ Page 6-4, paragraph 6-7b(6). Change to read 6-7b(5).
- ✓ Page 6-4, paragraph 6-7b(7). Change to read 6-7b(6).
- ✓ Page 6-5, paragraph 6-7b(8). Change to read 6-7b(7).

- ✓ Page 6-5, paragraph 6-8b. In the second sentence after "5247-R," delete: (or DD Form 398-2, or DD Form 1879), change to read: (SSBI or NAC request).
- ✓ Page 6-7, paragraph 6-13. Delete this paragraph.
- ✓ Page 6-7, paragraph 6-14. Change 6-14 to read: 6-13.
- ✓ Page 7-1, paragraph 7-1. In the last sentence delete "the billets and providing".
- ✓ Page 7-1, paragraph 7-2. Change the word "Billets" to read: Access.
- ✓ Page 7-1, paragraph 7-2(a). Change to read 7-2. Beginning of first sentence change "Billets" to read: Access. In the third sentence change "Billets" to read: Access. In the third sentence change the word "are" to read: is. Delete the fourth sentence in this paragraph.
- ✓ Page 7-1, paragraph 7-2(b). Delete this paragraph.
- ✓ Page 7-1, paragraph 7-2(c). Delete this paragraph.
- ✓ Page 7-2, paragraph 7-3(a). Add the subparagraph "b" after the first sentence. Add the subparagraph "(1)" after the first sentence. Delete the last sentence. Add : The proposed data of marriage along with any affiliation to any foreign national to include relationship and nationality must be included in the SSBI packet. Add: subparagraph (2) The Commander will prepare a memorandum indicating the affiliation to a foreign national and forward it along with the SSBI packet.
- ✓ Page 7-2, paragraph 7-3b. Change to read 7-3c, after the word "SBI", delete: within the past 5 years provided that, add the word: where. At the end of the last sentence add: since the SSBI was conducted.
- ✓ Page 7-2, paragraph 7-3c. Change to read 7-3d. In the second sentence change the number "13" to the number "10" and the number "14" to the number "12." Delete the third sentence.

- ✓ Page 7-2, paragraph 7-4. In the second sentence after the word "identified" delete the rest of the sentence.
- ✓ Page 7-3, paragraph 7-4a. After the word "retained" delete: in an authorized billet.
- ✓ Page 7-2, paragraph 7-4b. In the first sentence after the word "cases," delete the rest of the sentence and add the following: access is given for an extended period. In the second sentence after the word "warranted", delete the rest of the sentence. Delete the 5th sentence.
- ✓ Page 7-4, paragraph 7-5. In the last sentence delete the words: and an existing billet. In the same sentence delete the words: by the billet.
- ✓ Page 7-4, paragraph 7-6d. In the first sentence delete the word: billet. In the same sentence delete: in the same billet (double billeting).
- ✓ Page 7-5, paragraph 7-6e. After the word "a", delete the rest of the sentence. Insert the following: security awareness briefing yearly.
- ✓ Page 7-5, paragraph 7-6f. Delete this paragraph.
- ✓ Page 7-5, paragraph 7-9. Delete this paragraph.
- ✓ Page 7-5, paragraph 7-10. Delete this paragraph.
- ✓ Page 7-6, paragraph 7-11. Change to read 7-9.
- ✓ Page 7-6, paragraph 7-12. Change to read 7-10.
- ✓ Page 7-6, paragraph 7-13. Change to read 7-11. Delete the subparagraph 7-13e.
- ✓ Page 7-7, paragraph 7-14. Change to read 7-12.
- ✓ Page 7-7, paragraph 7-15. Change to read 7-13.
- ✓ Page 7-7, paragraph 7-16. Delete this paragraph.
- ✓ Page 7-7, paragraph 7-17. Change to read 7-14.

- ✓ Page 7-7, paragraph 7-18. Change to read 7-15.
- ✓ Page 7-7, paragraph 7-19. Change to read 7-16.
- ✓ Page 7-8, paragraph 7-20. Change to read 7-17.
- ✓ Page 7-9, paragraph 7-21. Change to read 7-18.
- ✓ Page 7-9, paragraph 7-22. Change to read 7-19.
- ✓ Page 7-9 and page 7-10, paragraph 7-22a. After the second sentence add the following: The investigative requirements falls under the 5-year regency requirement. In the third sentence after the second granted insert the following: type of investigation/date of investigation.
- ✓ Page 7-10, paragraph 7-23. Change to read 7-20.
- ✓ Page 7-10, paragraph 7-24. Change to read 7-21.
- ✓ Page 7-10, paragraph 7-25. Change to read 7-22. In the first sentence change the word "through" to "to" and after "ATZK-PTF-P" delete the rest of the sentence. In the last sentence after the word "office" add: , 731st Ordnance Detachment (EOD) Office and 703d Ordnance Detachment.
- ✓ Page 7-10, paragraph 7-26. Change to read 7-23.
- ✓ Page 8-4, paragraph 8-12a(4). Change 10 to read: 11. Change 11b to read: 12.
- ✓ Page 8-6, paragraph 8-15h. Delete the first sentence. In the second sentence change the word "This" to: CCF's.
- ✓ Page 8-6, paragraph 8-16. Add the subparagraph: 8-16e, Rule No 5: The individual has the opportunity for a personal appearance before an administrative Judge from the Defense Office of Hearing and Appeals (DOHA).
- ✓ Page 9-4, paragraph 9-7. Add: Paragraph 9-8 DEACTIVATING UNITS., Paragraph 9-8a. On Post transfers USAARMC Forms 1378, Standard Forms 312 and open casefiles should be transferred to the gaining

command security manager. Security Division should be notified of subject's whereabouts when appropriate. When possible, DA Form 5248-R should be updated and/or finalized prior to file transfer. Closed case files may be destroyed. Paragraph 9-8b. Open/closed case files and USAARMC Forms 1378 pertaining to personnel being assigned off the installation should be destroyed. Security Division should be provided reassignment orders when appropriate. DA Forms 5248-R should be finalized and reassignment orders added as an enclosure to the form. Standard Forms 312 should be forwarded to the gaining command security office. Paragraph 9-8c. Security Division should be notified in writing or telephonically of all pending request for security determination/investigations that can be canceled due to the change in mission and/or assignment. Paragraph 9-8d. DO NOT execute Security Termination Statements due to reassignment. Termination Statements should only be executed upon termination of employment (i.e. civil service/U. S. Army), administrative withdrawal of security clearance, revocation of security clearance, or contemplated absence from duty or employment for 60 days or more (AR 380-67, paragraph 9-204a). (NOTE: Standard Forms 312 have been rendered invalid due to unwarranted completion of the Security Debriefing Acknowledgment portion.

- ✓ Pages A-1 - A-2. Withdraw appendix A, insert new appendix A.
- ✓ Page B-1. Withdraw appendix B, insert new appendix B.
- ✓ Pages D-1 - D-6. Withdraw appendix D, insert new appendix D.
- ✓ Pages E-1 - E-2. Withdraw appendix E, insert new appendix E.
- ✓ Page F-3. Withdraw appendix F-2, insert new appendix F-2.
- ✓ Pages G-1 - G<sup>5</sup>. Withdraw appendix G-1, G-2, and G-3, insert new appendix G-1. *G-4 + G-5,*
- ✓ Pages I-1 - I-6. Withdraw appendix I, insert new appendix I.
- ✓ Page J-4, appendix J-3b. Change SF 50 to read: SF 52B.
- ✓ Page J-4, appendix J-3f. Change SF 50 to read: SF 52B

C1, USAARMC Pam 380-67 (12 Feb 98)

- ✓ Page J-5, <sup>paragraph (2)</sup> ~~appendix J-4c~~. In the second sentence after the acronym SSBI, add the following: or previous valid NACI, NAC, or ENTNAC.
- ✓ Pages L-1- L-2<sup>8</sup>. Withdraw appendix L, insert new appendix L.
- ✓ Pages M-1 - M-5. Withdraw appendix M, insert new appendix M.
- ✓ Pages O-1 - O-4. Withdraw appendix O, insert new appendix O.
- ✓ Pages R-1 - R-2. Withdraw appendix R, insert new appendix R.
- ✓ Page S-1. Withdraw appendix S, insert new appendix S.
- ✓ Pages T-1 - T-7<sup>8</sup>. Withdraw appendix T, insert new appendix T.
- ✓ Pages V-1 - V-7<sup>4</sup>. Withdraw appendix V, insert new appendix V.
- ✓ Pages Y-1 - Y-4. Withdraw appendix Y , insert new appendix Y.

2. Post these changes per DA Pam 25-40.

3. File this change in front of the publication.

FOR THE COMMANDER:



ROBERT L. BROOKS  
Director, Information Management

OFFICIAL  
WILLIAM E. MARSHALL  
Colonel, GS  
Chief of Staff

DISTRIBUTION:

B plus  
25 ATZK-PTF-P

## Security

### Personnel Security Program

**Summary.** This pamphlet contains policy guidance disseminated by the Department of the Army pending revision of AR 380-67. It also contains local policy and procedures for requesting security clearances and personnel security investigations, designation of sensitive positions, unfavorable administrative actions, reporting of unfavorable information, suspension of access, and outlines command responsibility. It is to be used in conjunction with Army Regulation (AR) 380-67, Personnel Security Program.

**Applicability.** This pamphlet applies to all military and civilian employees of units, staff sections, directorates, and activities assigned to this headquarters and tenant commands as delineated in their intraservice support agreement.

**Suggested improvements.** The proponent of this pamphlet is the Security Division, G3/Directorate of Plans, Training and Mobilization. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, USAARMC and Fort Knox, ATTN: ATZK-PTF-P, Fort Knox, Kentucky 40121-5000.

**Supersession notice.** This pamphlet supersedes all previous Intelligence Newsletters, USAARMC Policy Memos, and Personnel Security Update memorandums as identified in appendix A.

### Table of Contents

	Paragraph	Page
Chapter 1		
General Provisions		1-1
Purpose	1-1	1-1
Referenced Publications	1-2	1-1
Referenced Forms	1-3	1-1
Definitions	1-4	1-2
Chapter 2		
Program Management		2-1
General	2-1	2-1
Responsibilities	2-2	2-1
Reporting Requirements	2-3	2-4
Inspections	2-4	2-4

	Paragraph	Page
Advice and Assistance Visits	2-5	2-5
Automated Personnel Security Reports	2-6	2-5
Security Management System	2-7	2-6
Chapter 3		
General Policy		3-1
Appointment of Security Manager	3-1	3-1
Supplemental Personnel Security Procedures	3-2	3-1
Routing of Personnel Security Actions	3-3	3-1
Limited Investigations and Security Clearances	3-4	3-1
Cancellations	3-5	3-1
Suspense Dates	3-6	3-2
Local Records Check	3-7	3-2
Reporting Unfavorable Information	3-8	3-4
CCF Telephone Terminal	3-9	3-5
Citizenship	3-10	3-5
Designated Countries	3-11	3-6
Supplemental Questionnaires	3-12	3-7
Chapter 4		
Designation of Sensitive Positions		4-1
Section I		
General	4-1	4-1
Section II		
Civilian Positions		4-1
Criteria for Security Designation of Positions	4-2	4-1
Authority to Designate Sensitive Positions	4-3	4-1
Procedures for Obtaining Sensitivity Approval	4-4	4-2
Position Sensitivity Roster	4-5	4-2
Investigative Requirements	4-6	4-2
Procedures for Filling a Position	4-7	4-3
Determination of Eligibility for Selected Individual	4-8	4-3
Section III		
Military Positions		
Personnel Security Requirements	4-9	4-5
Clearance/Investigation Requests	4-10	4-6
Excess Positions	4-11	4-6
Authorized Document System	4-12	4-6

	Paragraph	Page
Chapter 5		5-1
Requesting Personnel Security Investigations		
Section I		
General		5-1
Investigative Requirements	5-1	5-1
Proper Execution of Forms	5-2	5-1
Review of Personnel Security Questionnaires	5-3	5-1
Section II		
Types of Investigation and Forms Required		5-1
Entrance National Agency Check	5-4	5-1
National Agency Check	5-5	5-2
National Agency Check and Written Inquiries	5-6	5-2
DOD National Agency Check and Written Inquiries	5-7	5-3
Single Scope Background Investigation	5-8	5-3
Section III		
Periodic Reinvestigations		5-3
Exceptions	5-9	5-3
Five Year Periodic Reinvestigation	5-10	5-4
Fifteen Year Periodic Reinvestigation	5-11	5-5
Downgrading Security Clearance	5-12	5-5
Failure or Refusal to Complete Periodic Reinvestigation	5-13	5-5
Identifying Periodic Reinvestigation Requirement	5-14	5-6
Section IV		
"Catch-em-in-CONUS" Program		5-6
"Catch-em-in-CONUS" Program	5-15	5-6
Eligible Candidates	5-16	5-6
Responsibilities	5-17	5-6
Chapter 6		
Requesting Personnel Security Clearance and Granting Access		6-1
Section I		
Requesting Security Clearance		6-1
Granting Authority	6-1	6-1
Limitations	6-2	6-1
Limited Access Authorization	6-3	6-1
When to Submit a Request for Security Clearance	6-4	6-2

	Paragraph	Page
Interim Security Clearance	6-5	6-2
Documentation in SIDPERS	6-6	6-2
Personnel Security Requirements for Reassignment	6-7	6-3
Personnel Security Requirements During Emergency Deployment Readiness Exercises	6-8	6-5
 Section II		
Granting Access		
Granting Access	6-9	6-6
Documentation of Security Clearance/ Access Authorization	6-10	6-6
Access Rosters	6-11	6-7
Verification of Security Clearance/Access Authorization for TDY Personnel	6-12	6-7
Administrative Downgrading	6-13	6-7
TOP SECRET Billet Control System	6-14	6-7
 Chapter 7		
Special Access Program		
		7-1
 Section I		
Sensitive Compartmented Information		
		7-1
 General		
SCI Billets	7-1	7-1
Investigative Requirement	7-2	7-1
Nomination Procedures	7-3	7-2
Transfer-in-Status	7-4	7-2
Indoctrination	7-5	7-4
Debriefing	7-6	7-4
Termination of Access	7-7	7-5
Marking Instructions	7-8	7-5
Review/Revalidation of Billets	7-9	7-5
	7-10	7-5
 Section II		
Nuclear Weapons Personnel Reliability Program		
		7-5
Governing Regulation	7-11	7-6
Investigative and Certification Requirements	7-12	7-6
Supplemental Guidance	7-13	7-6
 Section III		
Chemical Surety		
		7-6
Governing Regulation	7-14	7-7
Personnel Security Requirements	7-15	7-7
Status	7-16	7-7

	Paragraph	Page
Section IV		
Information Systems Security		7-7
Investigative Requirements	7-17	7-7
Criteria	7-18	7-7
ADP Surety Determinations	7-19	7-7
Unfavorable Administrative Action Procedures	7-20	7-8
Section V		
Access to North Atlantic Treaty Organization Classified Information		7-9
Investigative Requirements	7-21	7-9
Local Policy	7-22	7-9
Section VI		
Critical Nuclear Weapon Design Information		7-10
Governing Regulation	7-23	7-10
Required Security Clearance	7-24	7-10
Requests for Certification	7-25	7-10
Briefing and Debriefing	7-26	7-10
Chapter 8		
Unfavorable Administrative Actions		8-1
Section I		
Reporting of Unfavorable Information		8-1
Regulatory Requirements	8-1	8-1
Primary Responsibility	8-2	8-1
Definition	8-3	8-1
Sources	8-4	8-1
Reporting Procedures	8-5	8-2
Unauthorized Absence or Suicide	8-6	8-2
Information Monitored by Security Division	8-7	8-2
Release of Information	8-8	8-3
Security Manager Responsibility	8-9	8-3
Section II		
Suspension of Access		8-3
Governing Regulation	8-10	8-3
Purpose of Suspension of Access	8-11	8-3
Options Available to Commander	8-12	8-3
Procedural Guidance	8-13	8-4

	Paragraph	Page
Section III		
Unfavorable Administrative Action Procedures		8-4
Governing Regulation	8-14	8-5
Letters of Intent	8-15	8-5
Appeals and Reconsiderations	8-16	8-6
Security Managers Responsibility	8-17	8-7
Involuntary Separation	8-18	8-7
Chapter 9		
Continuing Security Responsibilities		9-1
Section I		
Evaluating Continued Security Eligibility		9-1
General	9-1	9-1
Briefing	9-2	9-1
Management Responsibility	9-3	9-1
Section II		
Security Education		9-2
Security Education Briefing	9-4	9-2
Nondisclosure Agreement	9-5	9-2
Foreign Travel Briefing	9-6	9-3
Termination Briefing	9-7	9-4
Chapter 10		
Safeguarding Personnel Security Investigative Records		10-1
General	10-1	10-1
Handling of Investigative Files	10-2	10-1
Requesting/Reviewing Investigative Dossiers	10-3	10-2
Disposition of Personnel Security Actions	10-4	10-2
Appendixes		
A. Superseded Documents		
B. Responsible Commanders		
C. Items to Include in SOP		
D. Inspection Checklist		
E. MOS/Occupational Speciality Requiring Security Clearance		
F. Local Record Checks		
F-1. Sample USAARMC Form 1947		
F-2. Location/Addresses to Obtain Local Record Checks		

- G. Sample Formats for Additional Information
  - G-1. Request for Mental Evaluation
  - G-2. Request for Drug/Alcohol Evaluation
  - G-3. Personal Financial Statement
- H. U.S. Citizenship Documentation
  - H-1. Acceptable Documents for Proof of U.S. Citizenship
  - H-2. Samples of Acceptable Documents
  - H-3. U.S. Vital Statistic Offices/Application Form
- I. Standard Subject Interview Worksheet
- J. Designation of Sensitive Positions
  - J-1. Criteria for Position Sensitivity Designations
  - J-2. Criteria for Designation of ADP Positions and Application of the Criteria
  - J-3. Detailed Instructions for Completing SF 52-B
  - J-4. Investigative Requirements
  - J-5. Position Sensitivity Designation Roster
  - J-6. Sample Format DD Form 2600
- K. Data Codes for Security Clearance Required and Position Personnel Security Requirement
- L. Supplemental Instructions for Completion of Investigative Forms
  - L-1. DD Form 398
  - L-2. DD Form 398-2
  - L-3. DD Form 1879
  - L-4. DD Form 2280
  - L-5. FD Form 258
  - L-6. SF 85
  - L-7. SF 86
  - L-8. SF 87
  - L-9. SF 171
- M. Instructions for Completion of DA Form 5247-R
- N. Sample USAARMC Form 1378 and Instructions
- O. Sample Formats for SCI Requests
  - O-1. SCI Billet Request
  - O-2. SCI Nomination Request
  - O-3. Request for Interim SCI/Compelling Need
- P. Excerpt From AR 50-5
- Q. Excerpt From AR 50-6
- R. Sample Formats for CNWDI Access and Briefing
  - R-1. Request for CNWDI
  - R-2. Briefing Certificate
- S. Examples of Reportable Information
- T. Instructions for Completing DA Form 5248-R
- U. Sample Formats Pertaining to Suspension of Access to Classified Information
  - U-1. Sample Memorandum for Personnel File
  - U-2. Sample Memorandum for Suspension of Access
- V. Statement of Rebuttal Guidelines
- W. TRADOC Form 227-R, Report of Foreign Travel
- X. DA Form 2962, Security Termination Statement
- Y. How to Request an Investigative File Through the Freedom of Information/Privacy Act

## Chapter 1

## General Provisions

1-1. Purpose. This pamphlet sets local policy and procedures for implementation of the Department of the Army Personnel Security Program. This pamphlet is designed to be used in conjunction with AR 380-67.

## 1-2. Referenced Publications.

a. AR 380-5, 25 February 1988, Department of the Army Information Security Program.

b. AR 380-19, 1 August 1990, Information Systems Security.

c. AR 380-67, 9 September 1988, The Department of the Army Personnel Security Program.

d. AR 600-85, 3 November 1986, Alcohol and Drug Abuse Prevention and Control Program.

e. AR 680-29, 1 March 1989, Military Personnel-Organization and Type of Transaction Codes.

f. DA Pamphlet 600-8, 25 February 1986, Management and Administrative Procedures.

g. DA Pamphlet 600-8-1, 1 August 1986, Standard Installation/Division Personnel (SIDPERS) Battalion S1 Level Procedures.

h. DA Circular 380-93-1, 30 September 1993, DA Implementing Instructions for the Classified Information Nondisclosure Agreement (NDA), Standard Form 312.

*C1*  
*12 Feb 1994*  
i. ~~Federal Personnel Manual Supplement 296-33, 30 April 1981, The Guide to Processing Personnel Actions.~~  
*DC of Pers. mg + June 1994*

j. USAARMC Pamphlet 600-8-1, 5 May 1992, Standard Installation/Division Personnel System (SIDPERS).

k. Security Management System (CSP/SQL Version), Standard Operating Procedure (SOP), Installation Support Module (ISM), 14 January 1991.

## 1-3. Referenced Forms.

a. DD Form 1966/2 (Record of Military Processing - Armed Forces of the United States).

b. TRADOC Form 227-R (Report of Foreign Travel).

c. Standard Form 312 (Classified Information Nondisclosure Agreement (NDA)).

d. USAARMC Form 1378 (Record of Personnel Security Clearance/Action).

e. USAARMC Form 1947 (Local Records Check).

1-4. Definitions.

a. Federal Service. Federal Service consists of active duty in the military service, 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 24 months.

b. Credible. Offering reasonable grounds for being believed.

## Chapter 2

### Program Management

2-1. General. To ensure uniform implementation of the DA Personnel Security Program throughout this command, program responsibility is centralized at the Security Division, G3/DPTM.

#### 2-2. Responsibilities.

a. The Chief, Security Division has staff responsibility for providing guidance, oversight, and development of policy and procedures governing personnel security matters within USAARMC & Fort Knox. The Chief, Personnel Security Branch, is functionally responsible for the administration of this program. Responsibilities include:

(1) Providing program management through issuance of local policy, operating guidance and oversight.

(2) Providing staff assistance to commanders/directors/chiefs and security managers in resolving personnel security matters.

(3) Conducting inspections of serviced activities for implementation and compliance with pertinent personnel security regulations and directives.

(4) Approving civilian positions designated as sensitive, maintaining a record of sensitive positions, and informing the servicing civilian personnel office (CPO) of any change in position sensitivity.

(5) Granting interim security clearances and suspending access.

(6) Reviewing and processing requests for personnel security determinations and investigations to Commander, U.S. Army Central Personnel Security Facility (CCF); Director, Defense Investigative Service (DIS); or Chief, Office of Personnel Management (OPM), as appropriate.

(7) Approving requests for waivers, under emergency conditions, of investigative requirements for appointment to a sensitive position, assignment to sensitive duties, or access to classified information pending completion of the required investigation.

b. The Civilian Personnel Officer, Civilian Personnel Office (CPO) is responsible for:

(1) Ensuring that no individual occupies a noncritical-sensitive or critical-sensitive position until such time as the appropriate investigative requirement is met.

(2) Initiating and monitoring until completion all National Agency Checks with Written Inquiries (NACI).

(3) Providing basic information to the Chief, Security Division, G3/DPTM on derogatory cases that come to their attention.

c. Commanders (as identified in appendix B), directors, or chiefs, staff offices are responsible for:

(1) Implementing personnel security provisions of AR 380-67 and this pamphlet.

(2) Appointing an individual, preferably the S2 or security manager, to perform personnel security functions.

d. S2/security managers are responsible for performing personnel security functions as outlined in AR 380-67 and this pamphlet. Specific function include:

(1) Assisting personnel in completing applicable investigative forms.

(2) Initiating requests for personnel security investigations.

(3) Reporting adverse information.

(4) Suspending an individual's access to classified information upon request.

(5) Requesting security clearances.

(6) Accepting previously granted security clearances.

(7) Conducting oversight visits or inspections of subordinate activities at least once every 2 years.

(8) Preparing written internal personnel security procedures applicable to subordinate elements of the activity. The procedures should include, but are not limited to, items outlined in appendix C.

(9) Maintaining a roster of civilian and military positions designated as sensitive.

(10) Initial, refresher, and termination security briefings.

(11) Maintaining records of personal foreign travel.

(12) Ensuring appropriate personnel within subject's chain of command/supervision are kept abreast of pertinent personnel security matters pertaining to their personnel (i.e., directorate security managers must ensure brigade S2/security managers are knowledgeable of all pending personnel security actions pertaining to members of their command and vice versa).

e. Immediate commanders/supervisors are responsible for:

(1) Designating sensitive positions.

(2) Assisting employees in obtaining help when they are experiencing personal problems which may affect their eligibility to perform sensitive functions.

(3) Reporting any information to the security manager that may affect an employee's ability to perform sensitive functions.

(4) Suspending access to classified information or temporarily removing an individual from sensitive duties.

(5) Including security responsibilities on the performance standards of military and civilian personnel who have access to classified information or perform sensitive duties. As well as making a statement on annual performance reports of how the employees perform their security responsibilities.

(6) Making a statement on requests for personnel security investigations regarding knowledge of any adverse information that may affect the subject's security status.

(7) Ensuring personnel report personal foreign travel to the security manager.

(8) Ensuring that all supervised personnel receive security education training and briefings as required for the proper performance of their assigned duties.

(9) Protecting personal information in investigative and other reports about the person.

f. Individuals are responsible for:

(1) Familiarizing themselves with pertinent security requirements pertaining to their assigned duties.

(2) Recognizing and avoiding personal behavior that could result in their ineligibility for a position of trust.

(3) Promptly reporting information of a security significance as identified in AR 380-67, paragraph 9-103b.

(4) Reporting personal foreign travel.

g. Co-workers are responsible for advising 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.

2-3. Reporting Requirements. MACOM reporting requirements of AR 380-67, paragraph 11-102, were rescinded. This change will be reflected in the next revision of AR 380-67.

2-4. Inspections.

*C1  
19/10/94*  
a. The Security Division will conduct announced personnel security inspections at least once every 2 years, ~~either through the Commanding General's Command Inspection Program (CG-CIP) or regular security inspections.~~ Spot checks and unannounced inspections will be conducted by a Security Division representative as deemed necessary. A copy of the inspection results will be maintained on file within the activity until the next comparable inspection.

b. All personnel performing personnel security functions will be expected to be thoroughly knowledgeable in their area of responsibility. Additionally, a representative sampling of individuals occupying sensitive positions will be queried concerning their knowledge of pertinent security regulations that pertain to their assigned duties and their awareness of the standards of conduct required of persons holding positions of trust. A representative sampling of personnel security actions previously submitted will also be verified against official records to determine accuracy and appropriateness.

c. A copy of the personnel security inspection checklist is provided at appendix D. This is not an all-inclusive checklist, but can form the basis for locally developed inspection checklist or self-evaluation guide.

d. Each activity commander/director shall ensure that personnel security program matters are included in their

administrative inspection program. Inspections will be geared down to the lowest element where sensitive functions are performed and will be conducted at least once every 2 years. A copy of the inspection results will be maintained on file within the activity and subject to review by a representative of Security Division.

2-5. Advice and Assistance Visits. The Security Division will conduct advice and assistance visits upon request or as needed. Courtesy inspections will be conducted upon request or as deemed appropriate by Security Division. Courtesy inspections or assistance visits will not be conducted once the activity has been officially notified of a forthcoming announced inspection.

2-6. Automated Personnel Security Reports.

a. The Fort Knox SIDPERS data base can be used to generate several local unique and DA standard SIDPERS reports related to the Personnel Security Program. USAARMC Pamphlet 600-8-1 provides a brief description of several reports which are available and guidelines relating to these reports.

*C/ 12/20/94*  
b. The automated Personnel Security Status Report (previously titled Security Clearance Roster) commonly referred to as the SC3 (unit report), SC4 (installation report), or SC5 (~~194th Armored Brigade report~~) as identified in USAARMC Pamphlet 600-8-1, was designed by Security Division to give security managers a "snapshot" picture of all data relating to an individual's personnel security status. The level of clearance (CLN), type of investigation/initiation date (INV INIT/DT), and type of investigation completed/date (INV COMP) pertaining to an individual as noted on the report are top fed by CCF. The S2/security manager provides the information to Personnel Automation Division, Adjutant General (AG) for entries to the Personnel Security Status (PSS) and to the Personnel Administration Center (PAC) for entries to the Field Determined Personnel Security Status (FDPS) and the Personnel Reliability Program Assignment Status (PRPA). This report is provided by the Personnel Automation Division, AG to Security Division and S2/security managers on a monthly basis. This report is used by Security Division to compare/verify requests for personnel security clearance/ investigation against the actual personnel security requirement for the position, as identified by the commander/director. The automated Personnel Security Status Report (SC3, SC4, or SC5) cannot and will not be used to grant access to classified information.

c. Information stored in the SIDPERS data base can be used to assist the S2/security manager in effectively managing their Personnel Security Program (i.e., to identify periodic reinvestigation requirements or aliens possessing a security clearance). Assistance can be obtained by contacting the Personnel Automation Division, 4-1834/1785.

2-7. Security Management System. The Security Management System is an automated system designed to provide the security managers with current information on military personnel as it relates to security clearances. The system is presently being tested within the Security Division and can be accessed by brigade level units upon request. To obtain full benefits of the system it should be used by the security managers of the directorates/staff offices; and security managers of the battalions/squadrons. However, until safeguards are developed which will limit access capabilities, the use of this system is restricted to brigade level units. The system provides the security manager with:

a. The capability to update certain security information for each individual on the installation data base without affecting SIDPERS data.

b. An automated file to maintain information about the case files for individuals.

c. The capability to input, store, and print DA Forms 5247-R and 5248-R.

d. The capability to input, store, update, and print DD Form 173 for selected personnel in BCT training.

e. A listing of suspense dates for individual security actions.

A copy of the Security Management System (CSP/SQL Version), Standard Operating Procedure (SOP), Installation Support Module (ISM), 14 January 1991, can be obtained by contacting Directorate of Information Management (DOIM).

## Chapter 3

### General Policy

#### 3-1. Appointment of security manager.

a. The head of each activity shall appoint, in writing, an official to serve as security manager per AR 380-5, paragraph 13-304. This official shall be responsible for the administration of an effective Personnel Security Program in that activity and possess, as a minimum, a SECRET security clearance based on an Entrance National Agency Check (ENTNAC) and be a commissioned officer, warrant officer, noncommissioned officer (NCO) (SFC or above), or DA civilian (GS-07 or above). A copy of the appointment will be provided to Security Division, G3/DPTM, ATTN: ATZK-PTF.

b. Requests to waive the minimum rank/grade requirements for designation of security manager will be forwarded to the Chief, Security Division.

3-2. Supplemental personnel security procedures. Written internal personnel security procedures must be established within each activity. These procedures should encompass instructions for its own staff and headquarters element as well as procedures to be followed by all subordinate elements. Personnel security procedures also need to be addressed in the field standard operating procedures of all deployable units. This is normally covered under OPSEC and encompasses all the security procedures used in a field element.

3-3. Routing of personnel security actions. All personnel security actions on military and civilian personnel will be processed through the Personnel Security Branch, Security Division, G3/DPTM (office symbol: ATZK-PTF-P).

3-4. Limit investigations and security clearances. Requests for personnel security investigations/security clearances will be limited to those that are essential to current operations or required for a specific Military Occupational Specialty (MOS)/occupational skill, and which are clearly authorized by AR 380-67. A list of sensitive MOS/occupational skills is at appendix E.

3-5. Cancellations. Personnel security actions shall be canceled when no longer required. Request for cancellations will include full identifying data, action requested, and the reason for the cancellation (i.e., deletion from CAP III assignment, transfer, or discharge). If the individual is being separated from active

add  
see CI, 12 Feb 96

duty, indicate the basis for the separation and whether the individual will have a reserve obligation or enter into the National Guard. Provide two copies of orders on individuals being transferred or discharged.

3-6. Suspense dates.

a. Suspense dates will be monitored and forwarded so as to reach the Security Division on the date due. Arrangements for an extension should be made with a representative of the Personnel Security Branch before the due date if a suspense cannot be met. A command memo will be sent on all overdue actions which cannot be obtained in a reasonable amount of time through S2/security channels.

b. Personnel security actions required in accordance with Centralized Assignment Procedures (CAP) III must be processed as expeditiously as possible. DA has imposed a 21-day suspense. This date cannot be extended. Reason for noncompliance with CAP III actions must be fully documented. CAP III actions are an item of command interest on TRADOC inspections.

3-7. Local Records Check (LRC).

a. Before processing various personnel security actions a check of the local records for pertinent adverse or derogatory information which might preclude granting of a security clearance or assigning an individual to a sensitive position must be completed. USAARMC Form 1947 (Local Records Check) will be used to record results. The completed checks will be maintained on file and available for inspection until requested action has been finalized. LRC can be no older than 60 days upon receipt of the action at Security Division, G3/DPTM. Any problems encountered with receiving results of LRC in a timely manner that cannot be resolved at the requestor's level shall be referred to Security Division. LRC consist of the following:

(1) Military Personnel Records Jacket (MPRJ) or Official Personnel File (OPF) will be screened by the S2/security manager or an authorized representative for records of punishment, reduction in grade, letters of indebtedness, absence without leave, or other unfavorable information. Page 4, items 38-44, SF 171 (Application for Federal Employment) must be specifically reviewed for any existing unfavorable information when reviewing a file pertaining to a civilian employee. MPRJ or OPF should also be reviewed for an existing certificate of clearance or record of an investigation having been previously completed or initiated; and to ensure there has not been a single break in Federal Service (active duty, ARNG, USAR, ROTC, Federal civilian employment, Federal contractor employment, or combination, thereof) exceeding 24 months since the investigation date shown on the certificate of clearance. Refer to

paragraph 1-4, this pamphlet, for current definition of "Federal Service." Service dates must be verified through enlistment/employment records maintained in the MPRJ or OPF. Dates reflected for basic pay entry date (BPED), basic active service date (BASD), or civil service computation date cannot be used as those are adjusted dates.

(2) Medical records will be screened by competent medical authority for indications of mental or emotional instability, drug or alcohol abuse, or any other factors which may require adjudicative action under the provisions of AR 380-67. Competent medical authority is defined in AR 380-67, paragraph 1-303.4, as a board-eligible or board-certified psychiatrist or clinical psychologist employed by or under contract to the U.S. military or U.S. Government.

(3) Military police and local intelligence files will be screened by authorized representatives of Law Enforcement Command/Provost Marshal (LEC/PM) and Security Division, G3/DPTM, respectively, if the person has been in the geographic area for more than 30 days. Records will be screened for mention of criminal and/or illegal conduct of any kind or information included in AR 380-67, paragraph 2-200.

(4) Unit records will be screened by the commander or an authorized representative for letters of indebtedness, pending unit punishment, or other unfavorable information which the commander determines may make the person unsuitable to hold a security clearance or placed into a position of trust.

(5) Finance records (optional) will be screened by the S2/security manager for recurring financial difficulties, letters of indebtedness, absent without leave or other unfavorable information.

b. If a LRC cannot be/is not accomplished, for example, records lost or the person has not been in the geographic area for more than 30 days, explain in your request for personnel security action.

c. A copy of USAARMC Form 1947 is provided at appendix F-1. Locations of pertinent records are provided at appendix F-2. The form must be typed or legibly printed and signed by the security manager or authorized representative. \* The term "no record," which is preprinted on the form, simply means there were no records pertaining to the individual on file within the activity being queried. This term is considered favorable if completed by Security Division, G3/DPTM (INTEL RCDS) or LEC/PM (PMO RCDS). A "no record" pertaining to medical and personnel records means the records could not be located. An attempt MUST be made to locate these records. If after an exhausting search, the record could not be located, a statement to that effect is required. If temporary files are established and reviewed, so state.

\* see C1, 12 Feb 94

d. These forms can be picked up at Student Text Supply and Publications, Directorate of Information Management (DOIM), Building 1810, and are not authorized to be reproduced by the requesting activity.

C1  
12 Feb 96

3-8. Reporting Unfavorable Information. When unfavorable information is reported on DA Form 5247-R, DA Form 5248-R, ~~DD Form 398-2, DD Form 1387-1, or DD Form 1387-2~~ complete detailed information must be provided to enable CCF adjudicators to make a final security decision. Failure to do so could add 60 days or more to the processing time. CCF's adjudication policy is outlined in AR 380-67, appendix I.

a. The questions provided below should be used as a guide in developing and reporting derogatory information. These questions are not all inclusive. In particular, you should expand each question, as appropriate, to include answers to the basic interrogatives; who, what, when, where, why, and how. Use the same approach when dealing with any other loyalty or suitability issue.

\*FINANCES

- How much does subject owe to each debtor?
- Was bankruptcy filed?
- What is the total amount involved in the bankruptcy?
- Was it Chapter 7, 11, or 13?
- What date was petition filed?
- What was the date the bankruptcy was discharged?
- Have letters of indebtedness been received? If so, provide a copy of each letter and subsequent counseling statement or related information.
- Did you include amount and check number of checks returned for insufficient funds?
- Did the subject redeem the dishonored checks?
- Have you forwarded all available documentation related to the situation?

\*DRUGS/ALCOHOL

- Did you include dates of usage?
- What was the frequency of use?
- What type(s) of drugs?
- Was subject arrested? What were the civilian and military arrest dates?
- What were the results of judicial/administrative disciplinary actions?
- Was rehabilitative treatment involved? What were the dates?
- Was subject a rehabilitative success or failure?
- Did you forward results of drug/alcohol screening (AR 600-85, paragraph 3-6)?

C1, 12 Feb 94

b. Processing time at CCF can be cut down by providing evaluations or statements with your initial personnel security action. For an individual with alcohol/drug abuse problems, an alcohol/drug evaluation is required; mental or emotional problems require a psychological/medical evaluation; financial problems require a complete financial statement, a listing of all debts with current status, and current DD Form 398.

(1) The only time you should wait for CCF to direct you to obtain an evaluation is when subject's current DA Form 873 is annotated "DOSSIER REVIEW REQUIRED FOR CRITICAL NUCLEAR DUTY." Such an annotation indicates subject's dossier contains unfavorable information which may be relevant to the current problem and should also be provided to the official examining the subject. If this is the case, after review of the dossier CCF will direct an evaluation be obtained.

(2) Samples of memorandums for an evaluation or financial statement are at appendix G.

3-9. CCF Telephone Terminal/DIS Liaison Office. Representatives of the Personnel Security Branch are the only individuals authorized to contact CCF or DIS.

3-10. Citizenship.

a. Proof of U.S. citizenship must be obtained before initial nomination for a security clearance. AR 380-67, paragraph B-4d, appendix B, lists the documents which are acceptable for proof of U.S. citizenship. A current list of acceptable documents and selected samples are identified at appendix H-1 and H-2, this pamphlet. Item 41c, DD Form 1966/5, August 1985 edition and item 29c, DD Form 1966/2, January 1989 (or subsequent edition) were included in the list of authorized documents by DA provided an acceptable document as outlined in AR 380-67 was used by the recruiter. There is no requirement to reverify the citizenship of personnel previously verified unless there is reason to doubt the authenticity of the document or information. Subsequent clearance actions can reflect "Citizenship confirmed via DA Form 873" when a CCF generated DA Form 873 reflecting a security clearance exists in the personnel file.

b. The commander/director is responsible and accountable for accurate verification of U.S. citizenship and for ensuring personnel verifying citizenship are adequately trained and effectively supervised in the review of citizenship documentation. The review of citizenship documentation can be delegated.

Certifying officials may be commissioned or warrant officers, NCOs in grade SFC and above, or DA civilians GS-07 and above. This function would normally be performed by the security manager/S2.

c. Double-check procedures must be implemented to confirm a soldier or civilian is, beyond reasonable doubt, a U.S. citizen. If there is any doubt as to the validity of the documentation provided, a request that DIS verify U.S. citizenship should be submitted.

d. Records must be maintained which specify who and what documentation was used to verify an individual's U.S. citizenship. The reverse side of USAARMC Form 1378 (Record of Personnel Security Clearance/Action) should be used to satisfy this requirement. Records will be maintained until the individual departs the activity.

e. Before acceptance and subsequent granting of access, be on the alert for the possibility of erroneously granted security clearances. Security clearances previously granted to immigrant aliens must be reissued as Limited Access Authorizations or administratively withdrawn, as appropriate. When there is any doubt as to citizenship status, i.e., DA Form 873 reflects place of birth as Panama City, FL; DA Form 2 reflects Panama City, Panama, proper certification should be obtained.

f. Locations considered by the Department of Defense (DOD) to constitute U.S. citizenship by native birth for security clearance purposes are identified in AR 380-67, paragraph 1-330. Citizens of the Federated States of Micronesia and the Republic of the Marshall Islands\* are also considered, for security clearance purposes, as though the individuals were native born U.S. citizens.

g. The Federal Government does not maintain copies of birth records of persons born in the U.S. or its territories. The state or territory where the birth occurred maintains the record. Addresses of the Office of Vital Statistics for each state and territory and the fees for certified copies of birth certificates as well as an application form is provided at appendix H-3.

h. Any legal questions concerning naturalization and citizenship requirements should be addressed to Legal Assistance, Staff Judge Advocate, 4-2771.

3-11. Designated Countries. AR 380-67, appendix H (List of Designated Countries) has been rescinded by the Office of the Secretary of Defense (OSD). All policies in AR 380-67 pertaining specifically to "designated countries" are also rescinded.

3-12. Supplemental Questionnaires. Supplemental questionnaires/ checklists used in support of the Personnel Security Program are prohibited with the exception of the questionnaire used by the Personnel Security Screening Program (PSSP). Guidance on conducting personnel security investigation (PSI) screening interviews is contained in AR 380-67, appendix G, although specifically oriented for the SCI prenomination interview, this guidance can be used for all PSI processing reviews. A sample subject interview worksheet using this guidance is provided at appendix I.

## Chapter 4

## Designation of Sensitive Positions

## Section I

## General

## 4-1. General.

a. Certain positions involve duties of such a sensitive nature that the misconduct of a person occupying such a position could result in an adverse impact upon the national security. These positions are referred to as sensitive positions. All DA civilian and military positions must be categorized according to security sensitivity and a suitability determination made before personnel are placed into sensitive positions.

b. Sensitive positions and duties are designated based on the types of duties performed by the individual occupying the position. This applies to military members and civilian employees. Designating positions does not involve the individuals who may currently occupy them. Instead, it involves the duties of the position, regardless of who may be selected for the position. The key is to identify the types of duties for the position. After that, the emphasis is on selecting people that meet the qualifications to be placed in those positions.

## Section II

## Civilian Positions

4-2. Criteria for security designation of positions. Each civilian position must be categorized as either nonsensitive, noncritical-sensitive, or critical-sensitive per AR 380-67, paragraph 3-101. The criteria to be applied in designating sensitive positions are identified in AR 380-67, paragraph 3-101 and appendix J-1 of this pamphlet. Specific criteria for assigning automated data processing (ADP) I, II, or III positions and how to apply the criteria is provided at appendix J-2 of this pamphlet.

4-3. Authority to designate sensitive positions. The responsibility to establish and categorize each civilian position lies with the hiring official. Nonsensitive positions need no formal approval. The ~~Chief Personnel Security Branch~~ is the approving authority for all positions designated as sensitive.

*cl,  
12 Feb  
96*

*CDR/Dir of your activity*

\* *see c1, 12 Feb 98*  
Once approved, the positions cannot be downgraded or reclassified without ~~\*prior written approval.~~ Personnel security requirements must be identified in the job description and job announcement as a condition of employment. \* SENSITIVE POSITIONS WILL NOT BE DOWNGRADED/RECLASSIFIED SOLELY TO AID THE RECRUITMENT OF SPECIFIC PERSONNEL.

4-4. Procedures for obtaining sensitivity approval.

a. Standard Form (SF) 52-B (Request for Personnel Action) will be used to obtain approval for all positions designated as sensitive. SF 52-B must be ~~submitted~~ *presented* in duplicate. Detailed instructions are contained at appendix J-3 of this pamphlet and a sample SF 52-B provided at appendix J-3, figure J-1.

b. Once approved, ~~\*a control number will be assigned by the Security Division.~~ The number will be placed in the right hand corner of the form. Any future actions pertaining to a previously approved position should be referred to by the control number that was assigned. A copy of the approved position designation must be maintained on file within the activity and available for review during inspections. \*

c. A representative of the Personnel Security Branch should be notified of all changes affecting approved sensitive positions as they occur (i.e. change of incumbent). Information reflected on the SF 52-B maintained by the requesting office as well as the Personnel Security Branch must be kept current at all times. This is an inspectable item.

4-5. Position sensitivity ~~roster~~ *roster*. A ~~record~~ *record* of sensitive positions will be ~~maintained~~ *maintained* by the security manager. ~~To assist security managers, the Chief, Personnel Security Branch will provide a roster of approved sensitive positions to each activity on a quarterly basis. The roster should be reviewed for accuracy and returned to Personnel Security Branch noting corrective action required. If there were no changes, a negative response is required. A copy of the roster will also be provided by the Personnel Security Branch to the Civilian Personnel Office. The security manager is responsible for providing a copy of this roster to activity personnel responsible for submission of personnel actions. A sample format of the roster is provided at appendix J, figure J-2.~~

4-6. Investigative requirements. Each civil service employee is subject to an investigation before appointment. The type of investigation required is determined by position sensitivity. The investigative requirement and the stage of initiation and/or completion of the required investigation before subject's

appointment, along with exception to policy, is outlined in AR 380-67, chapter 3, section II. This reference is quoted in part at appendix J-4. The Chief, Security Division or an authorized representative is the only authority to grant exceptions to policy UP AR 380-67, paragraph 3-204.

4-7. Procedures for filling a position. Once the positions within the activity have been designated as to the required sensitivity, it is the responsibility of the hiring official, in coordination with the activity security manager to ensure that the individual selected for a sensitive position meets the prerequisite investigation/clearance requirement to occupy that position. The following is a sequence of events and procedures which must be applied.

a. When a SF 52-B is generated to fill a position, the position sensitivity will be extracted from the Civilian Position Sensitivity Designation Roster.

b. Upon receipt of the SF 52-B from the requesting agency, CPO will cross reference information noted on the form reflecting position sensitivity with their copy of the roster. Discrepancies will be telephonically reported by the Staffing Specialist to Personnel Security Branch for verification.

c. CPO will provide the activity a list of eligible candidates for the position using DA Form 2600 (Referral and Selection Register). Candidates may or may not meet the position sensitivity requirement. Reasons for selection or nonselection cannot relate to personnel security clearance availability or appropriate investigation. It is up to the hiring official to coordinate with the activity security manager to ensure appropriate checks on the selected individual are completed per AR 380-67 or AR 380-19. The hiring official will note on the DA Form 2600 that coordination was made with the activity security manager. If the individual is not available for immediate placement due to additional required personnel security processing, a separate memo reflecting this will be attached to the DA Form 2600. The security manager's name will be noted on the DA Form 2600 along with the date of coordination (see appendix J, figure J-3).

4-8. Determination of eligibility for selected individual. The following action must be accomplished by the security manager and CPO before the individual is placed into a sensitive position.

a. Local record checks must be conducted, as appropriate, by the S2/security manager. The intelligence check may be obtained

telephonically by contacting Personnel Security Branch, 4-6741/1655.

b. Subject's Official Personnel Folder (OPF), or available documentation in the case of a new hire, must be reviewed by the S2/security manager for unfavorable information and the existence of a DA Form 873 and/or favorably completed National Agency Check and Written Inquiries (NACI)/Single Scope Background Investigation (SSBI), as appropriate. The S2/security manager must also ensure that there has been no break in Federal Service exceeding 24 months since the latest investigation date.

c. If an appropriate investigation has not been completed, a request for exception to policy will be prepared by the hiring official. The request for exception to policy must include name, SSN, position title and number, control number assigned to the sensitive position by Personnel Security Branch, date and results of OPF and intelligence records check, and justification.

(1) If the position is noncritical-sensitive and a NACI is required, the request for exception to policy will be attached to the DA Form 2600 and forwarded to CPO. CPO will remove the request for exception to policy from the DA Form 2600 and forward it to Security Division for approval. CPO will add as an enclosure to the request, SF 86 (Questionnaire for Sensitive Positions) as prepared by the subject, and any supplemental forms required for processing of a NACI by OPM.

(2) If the position is critical-sensitive the request for SSBI will be added as an enclosure to the request for exception to policy by the S2/security manager and forwarded to Security Division for approval. If approved, the position may be filled only when the NAC portion of the SSBI\* has been completed and favorably adjudicated.

see  
CI,  
12 Feb 98

d. When an exception to policy is granted, the following conditions will apply:

(1) Subject will be notified by CPO that employment is subject to favorable completion of requisite investigation and granting of a security clearance, if appropriate. A copy of the approved exception to policy and advisement of conditions of employment will be placed in employee's OPF pending granting of a final security clearance/completion of favorable investigation.

(2) Subject will not be allowed access to classified information until that activity security manager is officially notified in writing that a security clearance has been granted, if applicable.

e. To bring a selected individual on board, a favorable intelligence check and valid prerequisite investigation (or exception to policy) is all that is initially required. If a security clearance is required, the S2/security manager must submit a request for security determination IAW AR 380-67 to Security Division in a timely fashion. If any unfavorable information exists, the selected individual cannot be brought on board until a security determination is made.

f. If an exception to policy is granted, Security Division will notify the activity security manager/S2 and CPO, ATTN: R&P, in writing upon completion of the investigation.

### Section III

#### Military Positions

4-9. Personnel security requirements. All military positions will be reviewed by commanders and supervisors for personnel security requirements per DA Pam 600-8, chapter 9-30, procedure 9-20 and USAARMC Pam 600-8-1, pages 3-2 through 3-4. The same criteria identified for civilian positions can be used. Personnel security position requirements as defined below will be entered into the SIDPERS Authorized Strength File. The data codes are contained in AR 680-29, paragraph 3-9. A copy of these codes is provided at appendix K. Any questions concerning data entry to the SIDPERS data base should be directed to Chief, Personnel Automation Division, SIDPERS Section, G1/AG, 4-1834/1785.

a. Personnel security investigation required (PSIR). A one-character data code which describes the type of personnel security investigation needed for a specific duty function.

b. Position personnel security status (PPSS). A one-character data code which reflects the highest level of personnel security eligibility for access to classified defense information required for a specific duty position.

c. Position personnel security requirement (PPSR). A one-character data code which describes the unique personnel security requirement for a specific duty position. The purpose is to identify and communicate the age limit/recency requirements and/or scope of investigations for certain positions and/or scope of investigations for certain positions, and to identify nuclear, chemical, and ADP personnel reliability requirements for the position.

*C1,  
12 Feb 98*

~~4-10. Clearance/investigation requests. The Security Division will not process requests for security clearance/investigation if they are not in agreement with personnel security position requirements identified in the SIDPERS data base. If a change in the personnel security position requirement has been submitted to G1/AG but it is not reflected in the current SIDPERS roster or has not been entered in the data base, a copy of the transaction request should be forwarded along with the request for clearance/investigation.~~

4-<sup>10</sup>~~11~~. Excess positions. If a military member occupies a position which has been coded as excess, the personnel security position requirement cannot be entered in the SIDPERS data base. Requests for clearance/investigation for personnel occupying excess position should contain specific justification for the clearance/investigation, and indicate that the position occupied by the subject is excess. The same holds true for one time requirements pertaining to personnel who otherwise occupy positions with no personnel security requirement. If the clearance/investigation is to meet a school or temporary duty (TDY) requirement, the request will reflect this and include full justification.

4-<sup>11</sup>~~12~~. Authorization Document System. The Modified Table of Organization and Equipment (MTOE) and tables of distribution and allowances (TDA) provide the means for recording job related qualifications for duty positions in the authorization document system (AR 310-49). By properly documenting the personnel security positions requirements into the SIDPERS Authorized Strength File, military personnel will arrive at their duty station with the proper security clearance and investigation.

## Chapter 5

## Requesting Personnel Security Investigations

## Section I

## General

\* see  
C1,  
12 Feb 94

5-1. Investigative requirements for the three clearance categories (TOP SECRET, SECRET, and CONFIDENTIAL) are outlined in AR 380-67, paragraph 3-401. Before initiating a request for investigation, ensure that the subject of the investigation will have sufficient time remaining in the service or the position after completion of the investigation to warrant conducting it. ~~\* The average completion time to include security clearance determination is as follows: SSBI/NACI = 180 days; ENTNAC/NAC = 120 days.~~

5-2. Security managers will ensure that request forms and prescribed documentation are properly executed in accordance with detailed instructions which accompany each form, and AR 380-67, appendix C. Supplemental instructions for completion of investigative forms as well as samples of selected forms are provided at appendix L. The forms required for each type of investigation cannot be substituted. Forms should be typed. All copies must be legible. The original must not be part carbon copy. Copies may be reproduced and used instead of carbon copies.

5-3. Before submission of investigative forms the S2/security manager must conduct a thorough review of the personnel security questionnaires (PSQ), along with the subject, to ensure that all items are completed properly and are explained in sufficient detail and that the subject understands information requested and its importance. This review must clarify any questionable/unresolved information listed on the forms, correct or explain discrepancies, and ensure that the subject of the investigation provides full explanation, where applicable, on the PSQ or supporting attachments.

## Section II

## Types of Investigation and Forms Required

5-4. Entrance National Agency Check (ENTNAC). An ENTNAC is conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. This is accomplished by the

U.S. Army Recruiting Command. It is the responsibility of the G1/Adjutant General to ensure no soldier departs from initial entry training or One Station Unit (OSUT) site until results of the ENTNAC have been received and documented in the Military Personnel Records Jacket (MPRJ). An ENTNAC can be used as a basis for granting a SECRET or CONFIDENTIAL security clearance. An ENTNAC consists of the following forms:

*\* call*  
*cl. 12/5/94*  
a. ~~\* DD Form 398-2 (National Agency Questionnaire (NAQ)) - revised Mar 90 (or any future revision) - original plus one copy required.~~

b. DD Form 2280 (Armed Forces Fingerprint Card) - Original only.

5-5. National Agency Check (NAC). A NAC is initiated by the activity S2/security manager. It can be used as a basis for granting a SECRET or CONFIDENTIAL security clearance. A NAC consists of the following forms:

a. ~~\* DD Form 398-2~~ - Original plus one copy required.

b. FD Form 258 (Applicant Fingerprint Card) - 2 charts required.

5-6. National Agency Check and Written Inquiries (NACI). A NACI is conducted on each Federal Civil Service employee at the time of appointment. This is accomplished by the Civilian Personnel Office. A NACI will not be requested by CPO if the employee is to be placed into a critical-sensitive position (see paragraph 5-8, below), or the employee was subject of a previous Background Investigation (BI) or Special Background Investigation (SBI) and there is not a break in Federal Service greater than 24 months. Confirmation of a previously conducted investigation can be accomplished by contacting Security Division, G3/DPTM. A NACI consists of the following forms:

a. SF 85 (Questionnaire for Nonsensitive Positions) - original, or

b. SF 86 (Questionnaire for ~~Sensitive Positions~~ <sup>National Security Position</sup>) - original plus one copy.

c. SF 87 (Fingerprint Chart) - original.

d. SF 171 (Application for Federal Employment) - copy of the SF 171 which came with the Certificate of Eligibles or which was used to make the appointment.\*

5-7. DOD National Agency Check and Written Inquiries (DNACI) - will not be required until further notice.

5-8. Single Scope Background Investigation (SSBI). The SSBI replaced the BI and SBI and serves as the standard investigation to determine eligibility for access to TOP SECRET and Sensitive Compartmented Information (SCI). The SSBI is also used as the basis for appointment to critical-sensitive/special access positions, and other positions which previously required a BI or SBI. The SSBI is initiated by the S2/security manager and consists of the following forms:

*\*  
OK  
Cl,  
12 Feb 94*

a. DD Form 1879 (DOD Request for Personnel Security Investigation) - ~~revised March 1990 (or any future revision)~~ \* - original and three copies.

b. ~~DD Form 398 (Personnel Security Questionnaire (PSQ)) - revised March 1990 (or any future revision) - original and five single sided copies.~~

~~c. DD Form 398-2 (items 1-6 and 8) - original and one copy for subject's spouse, betrothed, or cohabitant (individual living in a spouse-like relationship with subject) and on foreign-born immediate family members over 18 years.~~

*C* d. FD Form 258 (Applicant Fingerprint Card) - two originals.

e. ~~For SCI access, request for waiver for SCI eligibility must accompany SSBI for subject with non-U.S. citizen relatives (reference AR 380-67, paragraph 3-501).~~

### Section III

#### Periodic Reinvestigations

5-9. Periodic reinvestigations will not be requested if the following conditions apply:

a. The subject is within 12 months of retirement (reference AR 380-67, paragraph 3-700d).

b. Access is only required during periods of mobilization. (Authorization for one-time access under emergency situations is addressed in AR 380-67, paragraph 3-407.)

c. The subject previously submitted an investigation which would satisfy the PR requirement through the U.S. Army Reserve or

National Guard. (NOTE: An original DA Form 873 reflecting the updated investigation must be obtained for placement in subject's OPF. This can be accomplished by submitting DA Form 5247-R to CCF. The type of investigation that was initiated and the specific U.S. Army Reserve or National Guard activity that requested the investigation should be annotated in the remarks section of DA Form 5247-R.)

5-10. Five year periodic reinvestigative requirement. There are certain categories of duty, clearance, and access which require the conduct of a PR every 5 years. The PR scope is outlined in AR 380-67, paragraph B-5, appendix B. It applies to military, civilian, contractor, and foreign national personnel occupying a critical-sensitive position, possessing a TOP SECRET clearance, or occupying a special access program position or whose MOS requires access to TOP SECRET and/or SCI.

a. Situations and requirements that necessitate reinvestigations are outlined in AR 380-67, paragraph 3-700. The PR requirement should be identified at the 4 years, 6 months point. The subject should be given the investigative forms with sufficient time to complete them and allowing for one extension, if necessary. The investigative packet should be submitted through Security Division to the Defense Investigative Service (DIS) not earlier than the 4 years, 9 months point and before 5 years from the date of the last investigation. PR must be submitted within the 5 year period or access is automatically downgraded to SECRET and SCI withdrawn.

*12 Feb 94*  
(1) The investigative scope of a PR will be 5 years, provided that the PR is submitted before the expiration of the latest BI/SBI. If the latest BI/SBI/SSBI is outdated (more than ~~5~~ 7 years old), an initial SSBI will be submitted and the ~~DD Form 398~~ will be completed to cover a 10 year scope. *SF 46, Items 4, 5, and 6 will*

(2) Individuals who have a prior BI and require access to SCI must submit an initial SSBI.

~~(3) Periodic reinvestigations for individuals in a nuclear (AR 50-5) or chemical (AR 50-6) personnel reliability program (PRP) are not required as long as the member remains under the continuing evaluation aspects of the PRP. This applies strictly to an individual's PRP qualifications and has no bearing on the requirements for a security clearance. If an individual in the PRP requires access to TS or to SCI, a PR is required if the BI/SBI or SSBI, nearing the 5-year anniversary.~~

b. Investigative forms required for a PR are the same as for the initial investigation with the exception of: \*

(1) ~~DD Form 398-2 is not required on the spouse, betrothed, cohabitant, or on foreign born immediate family members over 18 years of age, if previously submitted.~~

(2) ~~Fingerprint Charts.~~

\* ~~5-11. Fifteen year periodic reinvestigation requirement. The investigation period for personnel with SECRET access is established at 15 years. A PR must be submitted on all personnel who require SECRET access by virtue of duty position or MOS and whose last investigation is at least 15 years old. (There is no across the board requirement for officers to submit a SECRET PR.)~~ *\*see cl, 12 Feb 98*

\* ~~a. PR must be submitted within 30 days after the 15-year anniversary date or access is automatically downgraded to CONFIDENTIAL.~~

\* ~~b. A SECRET-PR consists of the following forms:~~

~~(1) DD Form 398-2 - original and five single sided copies.~~

~~(2) FD Form 258 - two originals if previous investigation was an ENTNAC. No fingerprint charts are required if a NAC, NACI, BI, SBI, or SSBI was conducted previously.~~

\* ~~5-12. Security clearance downgrade actions, as appropriate, will be submitted via DA Form 5247-R (Request for Security Clearance Determination) on all personnel who have a DA Form 873 (Certificate of Clearance and/or Security Determination), as well as clearance certificate issued by other DOD components, in their personnel file, but do not currently require access nor hold a military specialty requiring a security clearance, and whose investigation is outdated.~~

\* ~~a. Item 12 (Citizenship), DA Form 5247-R, does not need to be completed.~~

\* ~~b. Item 11 (Local Files Checks), DA Form 5247-R, does not need to be completed. Annotate in the "Remarks" section that local files checks were not completed.~~

5-13. Failure or refusal to complete PR.

a. An individual who refuses, or neglects, to submit the completed investigation packet for the PR, as requested, should be advised that refusal or failure to do so will result in the withdrawal of access to classified information and the revocation of security clearance. The revocation of a security clearance

could result in the removal of the civilian employee from the position requiring access to classified information and for the military employee a possible change in duty assignment and eventual change in MOS if access to classified information is necessary for performance in that specialty.

b. If the individual still fails to comply with the request to submit a completed investigative packet, access should be suspended and DA Form 5248-R (Report of Unfavorable Information for Security Determination) submitted per AR 380-67, chapter 8. DA Form 5248-R must include the reason(s) for nonsubmission.

5-14. Procedures will be established to identify PR requirements on all assigned personnel and to ensure the PR is submitted within the specified time period. A list of sensitive Military Occupational Specialties (MOS) and occupational skills is at appendix E.

#### Section IV

##### "Catch-em-in-CONUS" Program

5-15. The "Catch-em-in-CONUS" (CEIC) program is a program initiated by DIS as a measure to reduce personnel security investigation case completion time. The program targets subjects of investigation who are being reassigned overseas (excluding Hawaii) and who will require TOP SECRET security clearances at their new duty stations. The objective is to have DIS conduct subject interviews and complete local leads on those subjects before they depart the CONUS losing command.

5-16. Eligible candidates for the program are soldiers on whom a SSBI or SSBI-PR must be initiated for TS clearance and who are:

- a. Scheduled for an overseas PCS within 180 days.
- b. In a training status and scheduled for departure within 90 days.
- c. Scheduled to leave within 30-45 days for deployment of more than 60 days.

5-17. The losing command S2/security manager is responsible for notifying the Security Division of such cases and providing investigative documentation as soon as possible. Sufficient lead time should be programmed to permit accomplishment of the subject interview by DIS before the individual's departure. The security manager/S2 should provide information as to whether the soldier will be on leave or delay-enroute for schooling before reporting for their port call. Applicable dates and addresses should be provided in item 18, ~~DD Form 398~~.

12, DD Form 1879.  
5-6

C1  
12 Feb 99

## Chapter 6

Requesting Security Clearance  
and Granting Access

## Section I

## Requesting Security Clearance

6-1. The Commander, CCF is the sole authority authorized to grant, deny, or revoke Department of the Army personnel security clearances. The authority to grant interim security clearances within this command has been delegated to the Chief, Personnel Security Branch, Security Division, G3/DPTM. Policies governing security clearances are outlined in AR 380-67, section IV.

6-2. Requests for security clearances will be limited only to U.S. citizens who require access to classified information for mission accomplishment and the requirement <sup>for civilians have</sup> has been so identified in the Civilian Personnel Position Sensitivity Designation Roster, ~~or in the case of military personnel in the Personnel Security Status Report (SC3, SC4, or SC5).~~ Every attempt will be made to place personnel in sensitive positions who already qualify and possess the prerequisite security clearance.

6-3. Limited Access Authorizations (LAA).

a. Immigrant aliens and foreign nationals are not eligible for security clearances. Limited access authorization may be granted to non-U.S. citizens under the conditions outlined in AR 380-67, paragraph 3-403.

b. LAA as addressed in AR 380-67, paragraph 3-403 was amended by HQDA as follows. Authority to grant a final LAA is restricted to authorities listed in AR 380-67, paragraph F-1, appendix F. MACOM commander may grant interim LAA upon completion of the SSBI or PR. Only individuals employed by the U.S. Army will be nominated for an LAA. Exceptions must be approved by HQDA, ATTN: DAMI-CIS. DIS will open, process, and close cases per AR 380-67, appendix J and DIS 20-1-M. The completed SSBI or PR will be submitted by MACOM commander to CCF along with completed DD Form XX (to be signed by CCF), and DA Form 5247-R and justification including description of precise duties, nature of information accessed, and reason U.S. citizen can not fulfill duties. CCF will issue DA Form 3028-R granting LAA, or advise of cause for denial, and annotate DCII. MACOM commander will advise CCF when an existing LAA is terminated or not renewed. CCF will maintain a file containing completed DD Form XX for each active LAA.

CI  
12 Feb 98

6-4. When a person requires a security clearance and the following conditions exist, security managers will submit a request for security clearance utilizing DA Form 5247-R (Request for Security Determination). Requests for investigation for security clearances (DD Form 1879, ~~DD Form 398-2~~, and SF 86) do not require submission of DA Form 5247-R. Instructions for completing the form are contained in appendix M.

See Cl,  
12 Feb 98

a. No certificate of clearance or an invalid certificate of clearance is available in the person's personnel file. The following types of certificate of clearances are invalid:

- (1) Issued by organizations other than CCF.
- (2) Issued by CCF in noncomputer-generated mode.

(3) Final certificate of clearance issued on an interim basis by commander per authority of CCF to facilitate movement of trainees and students.

(4) Any other certificate of clearance reflecting a final clearance if not a CCF computer-generated form.

b. Prerequisite investigative and recency requirement as outlined in AR 380-67, paragraph 3-401 and section III, chapter 5, this pamphlet are met.

\* (1)  
(2)

c. The person has had no break in Federal service exceeding 24 months since the completion of the investigation.

d. The person can prove U.S. citizenship by presenting one of the documents listed in appendix G.

e. Significant derogatory information developed after the date of the last clearance is known.

6-5. Interim security clearances may be requested when an individual needs immediate access to classified information and meets the criteria listed in AR 380-67, paragraph 3-401. Requests for interim security clearances should be kept to a minimum and must contain full justification, date security clearance action required, and certification that no other properly cleared person is available on a temporary basis to accomplish the duties. No request for interim security clearance should be requested when unfavorable information is disclosed during review of local records.

\* b.

6-6. Documentation of Valid Security Clearances Contained in Local Personnel Files in The Total Army Personnel Data Base (TAPDB).

a. The TAPDB is the automated system of record for personnel security information. CCF is the single source for personnel security information in the TAPDB. CCF provides data directly (security clearances) or captures and forwards data from DIS (investigations). Data posted to the TAPDB is available immediately to field users through the Enlisted Distribution Assignment System (EDAS)/Total Officer Personnel Management Information System (TOPMIS), or on delayed basis through local SIDPERS which is updated by transactions generated when the TAPDB is posted by CCF. Every 60 days, each soldier will have the SIDPERS values for the security clearance granted by CCF and the investigation completed by DIS compared with the information indicated in the TAPDB. If there is a difference, a transaction will be generated to correct local SIDPERS.

b. When discrepancies are found in data contained in the SIDPERS Personnel File (SPF) and the DA Form 873 contained in the MPRJ, the following procedures will be used to reconcile the data:

(1) First, ensure that the SIDPERS Form (ORB, DA Form 2A or 2B) was dated a minimum of 60 days after the date that the DA Form 873 was issued. If the DA Form 873 is more recent than the SIDPERS form, then the latest clearance data was not present in SIDPERS when the form was generated and no action should be taken at that time.

(2) If the SIDPERS document is more recent, attach a copy of the DA Form 873 ~~and a copy of the SIDPERS form~~ to a DA Form 5247-R and forward them to Security Division, G3/DPTM. Do not forward DA Form 873 alone, ~~or SIDPERS documents alone~~; both are needed in order to resolve the discrepancy. To update the DA Form 2A the remarks section of the DA Form 5247-R should state "REQUEST DA TOP LOAD"; to update the ORB, the remarks section of the DA Form 5247-R should state "CORRECT ORB Security Data." If the update is time sensitive (i.e., promotion board, deployment, etc.), so indicate.

(3) Once a request is received at CCF, the DA Form 2A is normally updated within 3 working days. However, it takes up to 14 days for CCF to verify that the DA Form 2A for an active duty soldier has actually updated at PERSCOM. ORB updates are also completed within 3 working days of receipt.

(4) Security personnel will not receive any documentation from CCF verifying the reconciliation of data. Subjects should, therefore, be advised to contact their branch managers for a copy of the updated DA Form 2A or ORB.

6-7. Personnel Security Actions for Reassignment.

a. The Department of Defense in collaboration with the Joint Chiefs of Staff and the Army Vice Chief of Staff, put forth specific policy for processing personnel security actions required for reassignment. This policy dictates that personnel security actions required for reassignment will be submitted through appropriate channels to DIS or CCF, within 21 calendar days after reassignment instructions are received by Security Division, G3/DPTM.

b. This policy will be implemented as follows:

(1) All correspondence related to military personnel security actions for reassignment will be so identified and expeditiously processed. This includes conducting local records checks. Delays encountered during any phase of processing these actions will be fully documented and forwarded to Security Division (i.e., date, time, individuals involved, and problems encountered).

(2) Personnel Reassignment Section, G1/AG will provide Security Division a hard copy of each reassignment instruction requiring a personnel security action.

(3) The Security Division will notify the unit S2 of required personnel security action and date by which the action must be completed.

(4) The unit S2 will immediately initiate appropriate action and forward the completed action to Security Division. Credible derogatory information revealed during any phase of processing, which, in the opinion of the S2, would disqualify the individual for a security clearance/special access or reassignment, will be reported immediately to Security Division. Personnel Reassignment Section will be advised of the information by the Security Division and will, in consultation with Security Division, render a determination whether or not further processing is warranted.

*Cl,  
12 Feb 98*  
~~(5) S2 personnel are responsible for ensuring that a copy of the request for personnel security action is placed in the individual's MPRJ.~~

<sup>5</sup>  
~~(5)~~ Upon completion of the personnel security action, Security Division will forward the DA Form 873 to the requesting agency. The requesting agency is responsible for ensuring the form is then placed in subject's MPRJ before his departure.

<sup>6</sup>  
~~(7)~~ The Security Division will notify Personnel Reassignment Section upon completion of all security clearances required before the subject can ship.

7

(8) When reassignment instructions require the individual to be Personnel Reliability Program (PRP) qualified UP of AR 50-5 (Nuclear Surety) or AR 50-6 (Chemical Surety) Security Division will inform the appropriate S2, who will in turn ensure execution of DA Form 3180 (Personnel Screening and Evaluation Record).

#### 6-8. Personnel Security Requirements During Emergency Deployment Readiness Exercises (EDRE).

a. Personnel security requirements for participation in EDRE should be identified and incorporated into the unit's overall security posture to ensure the exercise is not compromised upon receipt of execution orders.

b. S2 personnel will ensure that all personnel participating in the exercise meet the prerequisite security clearance/investigative requirement, to include acceptance of a previously granted security clearance. A request for security clearance will be submitted to Security Division via DA Form 5247-R ~~(or DD Form 398-2 or DD Form 1879, as appropriate)~~ <sup>SSOI or NAC request</sup> during the required N-hour sequence on all personnel not possessing the prerequisite personnel security requirement. The top of each request for security clearance/investigation will be marked in red letters "IMMEDIATE ACTION REQUIRED FOR EDRE."

c. If a request for personnel security action was previously submitted, forward a copy of the original action with a notation in red on the top of each request stating "TRACER--IMMEDIATE ACTION REQUIRED FOR EDRE."

d. During EDRE, an interim security clearance will be granted by an authorized representative of Security Division pending verification of U.S. citizenship provided there is no reason to suspect the subject is not a U.S. citizen and all other provisions outlined in AR 380-67, paragraph 3-401 have been met. The subject will be instructed to obtain necessary documentation, and upon completion of EDRE, a request for final clearance will be submitted to Security Division.

e. During EDRE, there is no waiver of any requirements outlined in AR 380-67, with the exception of the waiver noted in subparagraph d, above. Personnel Security actions will be expeditiously processed by all concerned and oversight measures implemented to ensure an initiated action is completed during the designated N-hour sequence.

Section II

Granting Access

6-9. Accepting a Certificate of Clearance

a. Access to classified information can be granted to persons whose official duties require such access, and who have the appropriate personnel security clearance which has been accepted by the S2/security manager. Security managers can accept an existing valid (final security clearance issued by CCF in computer-generated mode) DA Form 873, Certificate of Clearance and/or Security Determination, per AR 380-67, paragraph 7-102b provided:

(1) There has been no break in Federal service exceeding 24 months since the investigation date; and

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

b. When the individual's personnel file contains a valid DA Form 873 and is absent of any unfavorable information, interim access to the appropriate level of clearance may be authorized up to 15 working days pending a check of the remaining local records. Access will be immediately discontinued upon receipt of credible adverse information. This exception to policy should be used only when a delay pending completion of the required local records will be harmful to mission accomplishment.

c. Access authorizations can be transferred from one U.S. Army Armor Center or School security manager to another. Clearance must be reaccepted before granting access to persons transferring from a tenant command.

d. The responsibility for determining whether an individual has an established need-to-know and the appropriate security clearance rests upon the individual who has authorized possession, knowledge, or control of the information.

6-10. Documentation of Security Clearance/Access Authorization.

a. An existing DA Form 873 is considered by this command as officially accepted upon signing and dating of USAARMC Form 1378, Record of Personnel Security Clearance/Action. Detailed instructions for completion of USAARMC Form 1378 is contained in appendix N. The FDPS element of the Personnel Security Status Report (SC3, SC4, or SC5) must be coded as appropriate, for military personnel authorized access to classified information.

b. USAARMC Form 1378 will be destroyed 30 days after Permanent Change of Station (PCS) or Expiration of Term of Service (ETS)/retirement of the individual. USAARMC Form 1378 will be forwarded to the gaining activity's S2/security manager in the case of on-post transfers.

6-11. Access Rosters. USAARMC Form 1378 is considered, in itself, an access roster. If a printed listing is prepared for use as an access roster it must contain as a minimum, subject's name (LAST, First, Middle initial), rank/grade, social security number, and degree of access authorized. Access rosters will be compiled and signed by the security manager utilizing USAARMC Form 1378 as the source document. Rosters will be kept to an absolute minimum consistent with operational necessity. All personnel maintaining a copy of the access roster will be informed of significant changes as they occur.

6-12. Verification of Security Clearance/Access Authorization for TDY Personnel.

a. Security managers shall establish internal controls to ensure assigned personnel requiring access to classified information while TDY are identified and appropriate action taken to obtain/accept the security clearance before departure. Internal controls must also be established to ensure the security clearance is not typed on travel orders (DD Form 1610, Request and Authorization for TDY Travel of DOD Personnel) unless written verification of the security clearance has been provided by the security manager. Some installations do not accept DD Form 1610 as a valid document for verifying security clearances; therefore, it is recommended that security clearance verification be passed to TDY locations by memorandum, message, or FAX.

b. Access to Sensitive Compartmented Information at the TDY site must be verified by the Special Security Office (SSO), G3/DPTM. Telephone numbers for the SSO are 624-5529/3135 (DSN 464-5529/3135).

*e1,  
12 Feb 98*  
~~6-13. Administrative Downgrading. Security clearances based on an outdated investigation will be forwarded to CCF via DA Form 5247-R for reissuance at the next lower level unless a request for periodic reinvestigation was forwarded to DIS before the anniversary date of the previous investigation. Periodic reinvestigations are addressed in section III, chapter 5, of this pamphlet~~

<sup>13</sup>  
6-14. TOP SECRET Billet Control System. The TOP SECRET billet control system required by AR 380-67, paragraph 3-104 is held in temporary suspension pending automation of the Total Army Authorization Document System.

## Chapter 7

## Special Access Programs

Special access programs are addressed in AR 380-67, sections V, chapter 3.

## Section I

## Sensitive Compartmented Information (SCI)

7-1. General. SCI allocations are controlled by the Assistant Chief of Staff for Intelligence, Department of the Army (ACSI-DA). The Chief, Special Security Office (SSO), Security Division, G3/DPTM is responsible for managing ~~the billets and providing~~ SCI access.

*Access*

## 7-2. SCI Billets.

a. *Access* Billet justifications should be forwarded to G3/DPTM, ATTN: ATZK-PTF-S in the format shown at Appendix O-1. The justifications must clearly establish a mission-related need for access to SCI material. *Access* Billets that ~~are~~ <sup>is</sup> requested for professional development of the incumbent will not be favorably considered. ~~Requests for additional billets will be disapproved if a billet previously allocated to the requesting activity is currently vacant in excess of 90 days with no previous record of active participation and utilization of the SCI program.~~

b. ~~Commander/director cannot internally redistribute assigned billets.~~

c. ~~The SSO will evaluate assigned unused billets. Any unused billet may be withdrawn by the SSO. The SSO will notify the existing activity in writing of the intent to withdraw a billet and will establish a suspense date for rebuttal. Billets subject to withdrawal are as follows:~~

(1) ~~A billet vacant for a period of 90 days for which no nominee has been identified or a justification for nonfill established (i.e., pending arrival of person from another command and required data not available).~~

(2) ~~An individual nominated for indoctrination who fails to complete necessary actions as directed (i.e., not submitting necessary security investigation forms).~~

C1,  
12 Feb 98

~~(3) A billet identified with a position undergoing a change in mission which no longer required access to SCI.~~

~~(4) An indoctrinated individual not using his access to special intelligence material for a period of 90 days.~~

7-3. Investigative requirement.

a. Personnel security standards identified in AR 380-67, paragraph 3-501a(1)-(6) should be reviewed before submitting a request for investigation and/or nomination. ~~On 23 December 1993 the spousal citizenship restriction in AR 380-67, paragraph 3-501a(5) was rescinded by the Deputy Chief of Staff for Intelligence. The spouse and intended spouse does not have to become, nor state an intention to become, a U.S. citizen. The revised AR 380-67 will reflect this change. Marriage to a foreign national will still be considered during the adjudicative process, but non-U.S. citizenship alone is unlikely to adversely affect an otherwise favorable review. The requirement for a compelling need statement, however, must still be submitted by a commander, LTC or above, certifying that a compelling need exists for the individual to have access.~~

<sup>c</sup> ~~b.~~ The investigative requirement for access to SCI is a SSBI or SBI conducted ~~within the past 5 years provided that there has been no break in Federal service greater than 24 months since the SSBI was conducted.~~

<sup>d</sup> ~~e.~~ If it is determined that the nominee does not possess a current SSBI or SBI, a SSBI packet (or SSBI PR, as appropriate) will be submitted to G3/DPTM, ATTN: ATZK-PTF-P for review and further processing. Place the number assigned to the billet in item ~~13~~<sup>10</sup>, DD Form 1879; justification should be indicated in item ~~14~~<sup>12</sup>. ~~The investigation and subsequent adjudication action can take up to 6 months to complete. To ensure effective utilization of assigned billets, the investigation should be submitted in sufficient time to allow for it to be completed before the billet becoming vacant.~~

7-4. Nominations procedures. Individuals requiring SCI access should be nominated as soon as they are identified ~~to fill an approved billet.~~ Nominations will be submitted through Personnel Security Branch to SSO in the format shown at appendix O-2.

a. Time remaining in a command or position is not a bar to submitting a nomination; however as a guideline, persons should not be nominated for access unless there is reasonable assurance that they will be retained ~~in an authorized billet~~ for at least 1 year from the date of indoctrination.

See c1, 12 Feb 98

b. In most cases, ~~an approved billet will exist before the incumbent is nominated for access.~~ Exceptions are nominations for one-time access to attend a conference or briefing, or other situations in which temporary (no more than 90 days) SCI access appears warranted, ~~but establishment of a permanent billet is not.~~ Normal SCI investigative standards apply in cases involving one-time access. Nominations for one-time access will be in the same format as shown at appendix O-2. ~~Billet number should reflect "One-time Access" and the remarks section must include justification for one-time access (where access is needed, why, how long, and point of contact at site).~~

c. All requests for exceptions to personnel security or investigation standards must clearly substantiate the existence of a "compelling need" per AR 380-67, paragraph 3-501c(2) and d.

(1) To minimize the need for the use of "compelling need" requests, command management procedures should ensure that SCI coded personnel requisitions are used for all individuals who will require SCI access.

(2) Commanders, LTC and above, must certify that a "compelling need" exists. When evaluating a compelling need the commander must balance the risk to national security against the gain to the mission and that the gain "far outweighs the risk." As part of this evaluation, the availability of other SCI eligible personnel must be determined. If no other personnel are available, and subject meets the criteria listed below, the commander may request, through SSO channels, that CCF grant subject interim SCI access eligibility. The nomination format for a compelling need request is provided at appendix O-3.

(a) Preparation and favorable review of an SSBI request.

(b) A favorable, prior personnel security investigation (PSI) (otherwise, you must wait for the NAC portion of the SSBI to close).

(c) Verification that the prior PSI is still valid (no break in service greater than 24 months since completion of the PSI).

(d) Favorable review of local files.

(e) Initiation of the SSBI (received by DIS).

(f) Compelling need for SCI access. AR 380-67, paragraph 1-303.3 defines a compelling need as: "Access to SCI which 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."

7-5. Transfer-in-status. SCI indoctrinated individuals will be debriefed from all SCI accesses when they leave their current organization for a position in another organization unless the gaining organization requests the individual remain indoctrinated. Gaining organizations may request the transfer based upon the existence of a need-to-know ~~and an existing billet~~ for the position the individual will occupy, and may only request the type of accesses required ~~by the billet~~.

C1,  
12 Feb 98

7-6. Indoctrination.

a. The nominated individual will be indoctrinated by SSO upon receipt of authorization from the CDR, CCF. A debriefing report from the losing command, via SSO channels, can also be used as authority to indoctrinate an individual for access to SCI.

b. The SSO will notify the activity security manager when a nominated individual is authorized for indoctrination and an appointment will be scheduled at that time. Incumbent will be instructed to report to the SSO, Building 1109-A, at the time scheduled for indoctrination.

c. At the time of indoctrination, the SSO will levy certain special requirements regarding travel and assignment restrictions, termination of access before PCS/ETS, along with the requirement to notify SSO (via activity security manager) of any significant change in personal status. Significant changes include, but are not limited to the following:

- (1) Change in marital status.
- (2) Legal name change.
- (3) Adverse involvement with law enforcement agencies, to include arrests for other than minor traffic violations.
- (4) Credit judgments, bankruptcy filings or repossessions.
- (5) Contact with foreign nationals.
- (6) Loss or possible compromise of classified information.

d. It is permissible during ~~billet~~ changeover to have the outgoing and incoming persons indoctrinated ~~in the same billet~~ ~~(double-billeting)~~ for a period not to exceed 90 days.

C1, 12 Feb 98

e. Individuals granted access to SCI will receive a ~~reindoctrination during the sixth month after initial indoctrination, and during the second year of the date of last indoctrination or SCI reindoctrination.~~ *Security awareness briefing yearly.*

f. Indoctrination ~~authority is only valid for 180 days.~~ It is therefore imperative that ~~indoctrination~~ is achieved in a timely fashion.

7-7. Debriefing. Appointment for debriefing must be coordinated with SSO when a person filling a billet no longer requires access, 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.

7-8. Termination of access. Whenever adverse or derogatory information concerning a person with current access to SCI is received, the SSO will be telephonically notified by the security manager with a written report via DA Form 5248-R submitted to G3/DPTM, ATTN: ATZK-PTF-P. The SSO is authorized to suspend access (not debrief) without obtaining advance authority from the CDR, CCF, if such action is based on the recommendation of Senior Intelligence Officer, G3/DPTM.

7-9. Marking instructions. ~~Under normal circumstances, a single billet justification or nomination will be marked FOR OFFICIAL USE ONLY. Two or more justifications or nominations coupled together will be marked CONFIDENTIAL and handled accordingly.~~

7-10. Review/revalidation of billets. ~~Commanders/Directors must ensure assigned SCI billets are fully utilized at all times. Any unused billets should be turned in. Once a year, activity security managers will be tasked to review assigned SCI positions to justify continuous need and usage. The following can be used as a means to determine this:~~

a. ~~Review duty description and justification to determine if duties can be performed without access.~~

b. ~~Identify what information is at the SCI level that is not available at the collateral level.~~

c. ~~Identify billets vacant in excess of 90 days.~~

Section II

Nuclear Weapons Personnel Reliability Program (PRP)

C1, 12 Feb 98  
9  
7-11. AR 50-5, Nuclear Surety, sets forth the policies, procedures, and responsibilities for implementing the Army Nuclear Surety Program.

10  
7-12. Investigative and certification requirements for personnel performing duties associated with nuclear weapons are addressed in AR 50-5, paragraph 3-6 (excerpt provided at appendix P) and in AR 380-67, paragraph 3-504.

11  
7-13. Supplemental guidance.

a. Service academy cadets are considered the same as active duty military when determining break in service. Reservists on active duty for training (ADT) and Reserve Officer Training Corp (ROTC) cadets are not considered to have been on active duty when determining break in service.

b. Policy clarification reference AR 380-67, paragraph 3-504a(2)(a) was rendered by United States Army Nuclear and Chemical Agency in that an ENTNAC does satisfy the investigation requirement for a controlled position even though it was completed for the purpose of first-term enlistment or induction into the Armed Forces.

c. Prerequisite security clearance/investigation for attendance at Phase I, EOD school is SECRET/SSBI. Students must arrive with a minimum clearance of INTERIM SECRET with a SSBI initiated. If subject does not possess the prerequisite clearance or investigation, two separate actions must be requested. DA Form 5247-R must be submitted to obtain the interim/final SECRET clearance; DD Form 1879 with accompanied applicable forms must be submitted to request the SSBI.

d. Request for dossiers should be submitted in memorandum format to Security Division, G3/DPTM, ATTN: ATZK-PTF-P. Memorandum must include subject's name (LAST, First MI), date of birth, state or country of birth, social security number and justification.

~~e. Security Division will monitor the status of the SSBI. If the SSBI is not completed within 150 days from the date the request was submitted to DIS, a DCII check will be conducted to ascertain the status of the investigation. Security Division will inform the requestor of the results of the DCII check.~~

Section III

Chemical Surety

12 C1, 12 Feb 98  
 7-14. AR 50-6, Chemical Surety, prescribes policies, procedures, and responsibilities for the Chemical Surety Program.

13  
 7-15. Personnel security investigations and clearance requirements are outlined in AR 50-6, paragraph 3-6. An excerpt of the regulation is provided at appendix Q. Minimum investigative requirement is an ENTNAC completed within the 5 year period immediately preceding initial assignment to a chemical duty position.

7-16. Status of the investigation will be monitored by Security Division. If the results are not received within 90 days of the date the request was sent to DIS, a DCII status check will be conducted and the requestor notified of results.

#### Section IV

#### Information Systems Security

14  
 7-17. Minimum investigative requirements for personnel performing ADP functions as outlined in AR 380-67, paragraph 3-614, and in AR 380-19, paragraph 2-17 are listed below. When completing applicable investigative forms ensure sensitive ADP (ADP I and II) requirements are indicated. USAARMC Form 1378 should be used to record sensitive ADP access eligibility.

a. ADP-I (critical-sensitive): Single Scope Background Investigation.

b. ADP-II (noncritical-sensitive): Entrance National Agency Check, National Agency Check, or National Agency Check and Written Inquiries.

c. ADP-III (nonsensitive): Entrance National Agency Check, National Agency Check, or National Agency Check and Written Inquiries.

15  
 7-18. Criteria for occupying an ADP I or II position are contained in AR 380-67, paragraph 2-200.

16  
 7-19. Suitability determinations:

a. Suitability determinations required prior to performing sensitive ADP functions are made by the commander/director based on the completed investigation and local records checks provided they are devoid of potentially disqualifying information. Potentially disqualifying information will be submitted for adjudicative action to the installation Information Systems Security Officer (G3/DPTM, ATTN: ATZK-PTF-I) in memorandum format. The memorandum will contain subject's full name, grade, SSN, position title and number,

sensitivity level, the control number assigned to the approved civilian position by Security Division, G3/DPTM, and contain the recommendation of the commander/director. The unfavorable information requiring adjudication will be added as an enclosure to the memorandum.

b. Before performing ADP III (nonsensitive) functions, the initiation of the prerequisite investigation must be verified. Local files checks are not required to be completed for personnel occupying ADP III positions. Persons suitable for hire are suitable to perform ADP III functions.

*c1, 12 Feb 98* <sup>17</sup> 7-20. Unfavorable administrative action procedures.

a. If the information present results in potential disqualification from the ADP Surety Program, the subject will be provided a written statement of the reasons why the unfavorable administrative action is being taken.

b. Potentially disqualifying information shall undergo a two level review by adjudicative officials, first, the Chief, Personnel Security Branch, and second the Chief, Information Systems Security Branch. When an unfavorable administrative action is contemplated, the letter of intent (LOI) must be approved and signed by the Chief, Security Division. The final notification of unfavorable administrative action, subsequent to the issuance of the LOI, will be approved and signed by the G3/DPTM.

c. When Security Division, G3/DPTM receives credible derogatory information and disqualification is considered appropriate, a letter of intent will be forwarded through the command security manager to the individual.

(1) The 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.

(2) The LOI will direct suspension of ADP duties.

d. The person concerned with be given the opportunity to reply in writing to the adjudication authority.

(1) The commander/supervisor 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 their intention of submitting a rebuttal.

(2) The commander/supervisor will ensure that the person is counseled as to the seriousness of the contemplated action and will offer advice and assistance needed in forming a reply.

(3) The person's response must address each issue raised in the LOI. Any written documentation may be forwarded. Letters of recommendation from supervisory personnel may be attached to the response. The response must be endorsed by the person's commander/director. The commander/director must provide recommendation and rationale.

e. Director, G3/DPTM's decision is considered final. This decision will be forwarded through the activity security office to the individual.

f. G3/DPTM's final letter of determination will state that if the person intends to appeal, the appeal must be submitted to Commander, USAARMC and Fort Knox, ATTN: ATZK-PTF-I, within 30 days from receipt of the letter. The security manager 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 completed.

#### Section V

#### Access to North Atlantic Treaty Organization (NATO) Classified Information

*C1, 12 Feb 98*  
<sup>18</sup>  
7-21. Investigative requirements for personnel assigned to NATO staff positions and personnel not assigned to NATO staff positions, but requiring access to NATO COSMIC, SECRET, or CONFIDENTIAL information are outlined in AR 380-67, paragraph 3-505.

<sup>19</sup>  
7-22. Local policy for access to NATO information is established by the Director, Directorate of Information Management (DOIM). Any specific questions pertaining to access of NATO information should be directed to DOIM Classified Files, 4-7425. Policy as set forth by DOIM is as follows:

*See C1, 12 Feb 98*  
a. Personnel will be briefed and cleared for access to the degree of NATO classified information which they have a need-to-know in the performance of their duties. Personnel must first possess the equivalent U.S. security clearance, and it must be locally accepted at the level of NATO classified information required. \* Before receiving the NATO briefing, the activity security manager/S2 will prepare a written request to DOIM Classified Files, ATTN: ATZK-IMO-R. The request will give the

See C1,  
12 Feb 98

name of the individual, social security number, degree of U.S. security clearance/date granted, degree of local access/date granted,\* and justification. Upon receipt of the request, the NATO Control Officer will contact the security manager and set up an appointment for the briefing.

b. A formal NATO briefing is required for access to NATO material classified NATO CONFIDENTIAL (NC) and higher. A formal briefing is not required for access to NATO RESTRICTED, however the individual must be instructed in the proper procedures for handling NATO material. The governing regulation is AR 380-15 (NC) Safeguarding Classified NATO Information (U).

c. Each individual with access to NATO CONFIDENTIAL or higher must be debriefed by the NATO Control Officer when access is no longer required or before termination of employment, administrative withdrawal of security clearance, revocation of security clearance, or contemplated absence from duty or employment for 60 days or more.

Section VI

Critical Nuclear Weapon Design Information (CNWDI).

<sup>20</sup>  
7-~~23~~. Policy for access to and dissemination of CNWDI is outlined in AR 380-150, Access to and Dissemination of Restricted Data. CNWDI is extremely sensitive and access must be limited to the minimum number of persons who need it to accomplish their assigned mission.

<sup>21</sup>  
7-~~24~~. The minimum security clearance for eligibility for access is final TOP SECRET or SECRET, as appropriate.

<sup>22</sup>  
7-~~25~~. Requests for CNWDI certification will be forwarded <sup>to</sup> through Commander, USAARMC & Fort Knox, ATTN: ATZK-PTF-P, ~~to Commander, TRADOC, ATTN: ATBO-JC, Fort Monroe, VA 23651-5000.~~ Requests will include information as noted in the sample format provided at appendix R-1. Commander, 43d Ordnance Detachment (EOD) Office\* will forward requests for CNWDI certification on assigned personnel directly to their higher headquarters.

See C1,  
12 Feb 98

<sup>23</sup>  
7-~~26~~. Briefing and debriefing will be executed by the security manager per AR 380-150. Sample briefing certificate is provided at appendix R-2. A copy of the Security Termination Statement and Debriefing Certificate, DA Form 2962, will be forwarded to G3/DPTM, ATTN: ATZK-PTF-P.

## Chapter 8

### Unfavorable Administrative Actions

#### Section I

##### Reporting of Unfavorable Information

8-1. Regulatory requirements for reporting of unfavorable information are outlined in AR 380-67, paragraph 8-101.

8-2. All personnel within the supervisory chain have primary responsibility for the continual monitoring of their personnel and reporting credible derogatory information which reflects on the suitability of the individual to hold a security clearance, to be placed in a position requiring a trustworthiness determination, or to be considered for security clearance at a future date.

8-3. Derogatory information is defined as information of such a nature as to constitute a possible basis for taking an adverse action. AR 380-67, paragraph 2-200, defines derogatory information by example. An abbreviated version is provided at appendix S. When derogatory information of a nature not specifically mentioned in paragraph 2-200 is discovered, and if it is considered to be credible derogatory information this information will also be reported.

8-4. Derogatory information can be obtained from many sources and must be coordinated with the S2/security manager to ensure appropriate reporting is accomplished. Some examples are:

- a. Military Police Desk Blotter and Reports;
- b. Serious Incident Reports (SIR);
- c. Criminal Investigation Command (CID) reports (obtainable under the provisions of AR 190-45);
- d. Enrollment in Alcohol and Drug Abuse Program (obtainable under the provisions of AR 600-85 and AR 40-66) and/or alcohol/drug related incidents;
- e. Letters of indebtedness and/or dishonored check notifications;
- f. Punitive actions (Articles 15, Court Martials, etc.);

- g. Adverse discharge/separation actions;
- h. Treatment for mental or nervous disorder or emotional instability; and
- i. Disqualification from a personnel surety program.

8-5. Derogatory information surfaced at the local level on assigned/attached military and DOD civilian personnel must be reported as it becomes known.

a. The vehicle used for reporting credible derogatory information is DA Form 5248-R (Reporting of Unfavorable Information for Security Determination). All reports will include full identifying data on the person. Extreme caution should be exercised to ensure the information reported is complete and accurate. Instructions for completing DA Form 5248-R are provided at appendix T. AR 380-67, appendix I, contains guidelines to assist DOD personnel security adjudicators in making determinations with respect to an individual's eligibility for employment, retention in sensitive duties, or access to classified information. Disqualifying factors as well as mitigating factors contained in AR 380-67, appendix I should be reviewed before submitting a final report to ensure all information required to make a final adjudication has been provided.

b. If the subject possesses a security clearance follow-up reports will be submitted to Security Division at intervals not exceeding 60-days until all pending actions are resolved.

c. If the individual DOES NOT possess a security clearance, the initial report will include in item 11b, DA Form 5248-R any and all action taken by the commander or appropriate authorities to resolve the incident. Item 11b, DA Form 5248-R, must also include an approximate date that the command action will be completed. A follow-up and/or final report will not be expected at Security Division until that date. If an approximate date is not provided, a follow-up/final report will be due within 60-days of the date of the report.

8-6. When an individual who has had access to classified information is on unauthorized absence or attempts/commits suicide, an inquiry will be conducted IAW AR 380-5, paragraphs 6-110 and 6-111, to detect if there are possible security implications. The results of the inquiry will be included in your report of unfavorable information.

8-7. Security Division, G3/DPTM monitors derogatory information which is available to them and the command group through the

Military Police Desk Blotter, Serious Incident Reports, and CID reports. If a reportable incident is not submitted to Security Division within 30 days of the date of the report, a request for the information will be sent to the activity with a 10 working day suspense.

8-8. Reports of unfavorable information should be released only to those individuals whose official duties necessitate a "need-to-know." A "need-to-know" includes, in the case of military personnel assigned to sensitive positions outside command channels, the sharing of reports of unfavorable information with the appropriate directorate/staff office security manager.

8-9. S2/security manager must ensure key personnel are familiar with indicators of personnel security concern, their responsibilities for reporting adverse information, and the appropriate procedures within their activity for reporting adverse information.

## Section II

### Suspension of Access

8-10. Suspension of access to classified information is addressed in AR 380-67, paragraph 8-102.

8-11. Suspension of access is an administrative action taken to protect the interests of national security and the command. It is not to be used as a disciplinary tool, nor viewed in that manner. Suspension of access is only appropriate when used in the best interest of national security. Access will not be suspended for frivolous, isolated, one-time incidents that appear unlikely to be repeated. Inappropriate suspension deprives the commander/supervisor of an otherwise useful individual and may unnecessarily deprive the individual of assignments, promotions, or other favorable personnel considerations.

8-12. The commander/head of the organization or an authorized representative shall determine whether or not suspension of an individual's access to classified information is warranted. Options pertaining to suspension and supplemental procedures are as follows:

a. Informal suspension can be used as an interim measure while gathering information to determine whether formal suspension is warranted.

- (1) Access may be reinstated by suspending official.
- (2) DA Form 873 is NOT removed from the personnel file.

(3) A final decision as to whether formal suspension is warranted must be rendered within 30 days.

*C1, 12 Feb 98*  
(4) If DA Form 5248-R is prepared before a final decision, item ~~10~~<sup>11</sup> should reflect "access NOT suspended" and in item ~~11b~~<sup>12</sup> indicate "Subject's access was suspended on an informal basis."

b. Formal suspension should be taken when information exists which raises serious question as to subject's ability or intent to protect classified information.

(1) Local access may not be restored until a final favorable determination is made by the CDR, CCF. If the commander requires the individual to have access before receipt of CCF's determination and all criteria outlined in AR 380-67, paragraph 8-102b is met, a written request for reinstatement along with full justification should be forwarded through command channels to Security Division, G3/DPTM.

(2) DA Form 873 MUST be removed from the personnel file and attached to the DA Form 5248-R. A memorandum should be placed in the personnel file showing removal of the DA Form 873. Sample memorandum format provided at appendix U-1.

8-13. Upon suspension of access, the S2/security manager must:

a. Notify the individual concerned in writing that access to classified information has been suspended and the reasons for the suspension. A sample format is provided at appendix U-2.

b. The individual's name must be deleted from all access rosters (USAARMC Form 1378 must be removed from the active file, lined through, and a notation made as to suspension of access). In the case of formal suspension pertaining to military personnel, appropriate FDPS Clearance Status SIDPERS transaction per DA Pamphlet 600-8-1, procedure 2-12, must be made to report change in local access (code "M" applies). Internal operating procedures must be established to guarantee all appropriate personnel are notified of the suspension action to ensure no inadvertent disclosure of classified defense information. Pending final determination, subject will be relieved of all sensitive duties.

### Section III

#### Unfavorable Administrative Action Procedures

8-14. Unfavorable administrative action procedures are addressed in AR 380-67, section II.

8-15. 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 (LOI) through Security Division, G3/DPTM to the individual.

a. A representative of the Security Division will present the letter of intent to the individual concerned. Arrangements to serve the individual with the LOI will be coordinated with the activity security manager. If access to classified information was not previously suspended, the Security Division will direct the security manager to suspend access.

b. Security Division will counsel the individual as to the seriousness of CCF's contemplated action and inform the individual of the option of submitting a letter of rebuttal. The individual will be advised that assistance can be obtained from Legal Assistance, Staff Judge Advocate or other lawyers (at the individual's expense), or from their unit commander/supervisor and activity S2/security manager, as well as Security Division.

c. If the individual intends to submit a rebuttal he or she will be instructed to route the rebuttal through the appropriate chain of command to Security Division within 50 days of receipt of acknowledgment. The response must address each issue raised in CCF's LOI and should include supporting documentation and recommendations from supervisory personnel as well as character testimonials, if available. The individual will be provided written guidelines for preparation of the statement of rebuttal as well as applicable excerpts from AR 380-67, appendix I. A copy of the rebuttal guidelines is provided at appendix V.

d. A copy of the LOI will be provided through security channels to the subject's unit commander or supervisor in the case of a civilian employee. A copy will also be furnished the duty station security manager, as applicable, for those soldiers assigned to Company A and B, USAARMC. The commander/supervisor will be informed whether the individual chose to submit a letter of rebuttal. If the individual submits a letter of rebuttal, the commander/supervisor must review the subject's rebuttal and provide a recommendation as to whether the person's security clearance should be denied, revoked, or restored. The commander/supervisor must provide rationale, addressing the issues outlined in the LOI and include information noted below:

(1) Length of time the commander/director has known the person.

(2) Indicate whether the person has or has not taken any steps to change the conduct or behavior.

(3) Personal knowledge of the person's character traits.

(4) Any other information which tends to show whether the person is or is not a security risk.

e. Response to LOI will be routed through command/supervisory channels. The S2/security manager is responsible for monitoring the action and ensuring the suspense date is met. Response to LOI that does not include the commander's recommendation will be returned.

f. S2/security manager will ensure that appropriate action is taken to suspend subject's access to classified information if action was not previously taken.

g. Command emphasis must be placed on timely submission of statements of rebuttal. Commander's should emphasize the seriousness of the contemplated action to the individual concerned and render assistance.

h. CCF's decision will be rendered within 90 days. <sup>CCF's</sup> ~~This~~ decision will be forwarded through Security Division to the individual.

c1,  
12 Feb 98

8-16. Procedural guidance for requests for appeals and reconsiderations are addressed in AR 380-67, paragraphs 8-201d and 8-201.1, respectively. Requests must be submitted through Security Division, G3/DPTM. The rules concerning appeals and reconsiderations are as follows:

a. Rule No. 1: Reconsideration requests go to CCF; appeals go to HQDA (DAMI-CIS).

b. Rule No. 2: If the subject of the action is providing additional information for consideration, it is a reconsideration request.

c. Rule No. 3: The commander (LTC or above), or supervisor (GS-13 or above) of the individual must provide the recommendation and rationale to revoke or reinstate the individual's clearance and/or SCI access. The action does not have to follow command channels after the commander or supervisor adds the recommendation.

d. Rule No. 4: Appeals are reviews of the existing record and only consider the information that was previously reviewed by CCF.

see c1,  
12 Feb 98 e. \*

8-17. The S2/security manager has an obligation to assist the individual by ensuring that the procedures are understood and followed, and by reviewing the packet before submission to make sure it addresses the issues and complies with procedures.

8-18. Involuntary separation of soldiers and DA civilian personnel. AR 380-67, paragraph 8-201.2 is revised as follows.

a. Before involuntarily separating employees who have had access to highly classified information, an evaluation must be made as to the risk of these employees improperly disclosing classified information. Employees who have had access to the following classified programs must be evaluated.

- (1) Sensitive Compartmented Intelligence (SCI).
- (2) Special Access Programs (SAP).
- (3) Critical Nuclear Weapons Design Information (CNWDI).
- (4) TOP SECRET cryptographic material.
- (5) TOP SECRET plans.
- (6) Nuclear PRP.
- (7) Presidential support.
- (8) Single Integrated Operation Plan-extremely sensitive information (SIOP-ESI).
- (9) Other programs of security interests.

b. In making the evaluation, management (minimum field grade officer or DA civilian equivalent) should base its initial assessment on the attitude displayed by the affected individual (i.e., display of anger toward the U.S. Army, resentment or perceived mistreatment). If there is a reasonable basis to believe that the individual may improperly disclose classified information in retaliation for separation, documentation as described below must be provided to HQDA (DAMI-CIS) through Security Division via the most expeditious means. Security Division will provide TRADOC a copy of all documentation forwarded to HQDA. Concurrent coordination with supporting medical staff should be effected to arrange for an evaluation. Processing of a separation for cause will be delayed pending resolution of the security issue.

c. Documentation required:

(1) Full personal ID data (include DPOB, MOS/branch/career/code, marital status, etc.).

(2) Length of service/total career time, eligible for reserve/national guard or other Federal employment.

(3) Type of discharge/dismissal contemplated and reason for same.

(4) Access level, scope of access and recency.

(5) Rationale supporting determination that separation may be detrimental to security.

(6) POC, address (mail and message), phone and fax (commercial and DSN).

d. The vast majority of personnel separated from service, including those involuntarily separated, are not security risks. The small number of personnel who may feel compelled to retaliate for a perceived wrong is the concern and purpose of this policy.

## Chapter 9

## Continuing Security Responsibilities

## Section I

## Evaluating Continued Security Eligibility

9-1. The procedures for evaluating continued security eligibility are outlined in AR 380-67, chapter 9. Commanders and security managers must ensure that managers, supervisors, individuals, and co-workers are thoroughly briefed and understand their responsibility in regard to reporting matters of personnel security concern.

9-2. All assigned individuals will be briefed on personal problems or situations that could affect their eligibility to be placed in or remain in a position of trust. Standards of conduct required of personnel holding positions of trust are outlined in AR 380-67, paragraphs 2-101 and 2-102. Criteria for application of security standards are outlined in AR 380-67, paragraph 2-200. Briefings should be designed so all personnel will be able to recognize and avoid the kind of behavior that would render one ineligible for, or continued assignment in, a position of trust. Common examples should be used to further explain criteria (i.e., dishonored checks, driving while intoxicated or under the influence, marijuana usage).

9-3. Commanders/supervisors:

a. Will encourage individuals cleared under AR 380-67 to seek appropriate guidance and assistance on any personal problem or situation that may have a bearing on their eligibility to remain in a position of trust.

b. Must include security responsibilities on the performance plans of military and civilian personnel who have access to classified information. Additionally, a statement will be made on the person's annual performance report describing how the security responsibilities were discharged and whether or not the supervisor is aware of actions, behavior, or conditions that would constitute a reportable matter under AR 380-67 and, if the response is affirmative, whether or not an appropriate report has been made.

(1) Recommended entries for inclusion in performance plan:

JOB ELEMENTPERFORMANCE STANDARDS

Application of security standards of conduct.

Recognizes and avoids personal behavior as outlined in AR 380-67, para 9-103 that may reflect adversely on incumbent's ability to safeguard classified information.

Discharge of security responsibilities. Safeguards classified information IAW AR 380-5 and other pertinent security directives.

(2) Bullet examples for annual performance report:

- o Properly safeguards classified and sensitive information
- o Handles personnel security records with the highest discretion
- o Maintains high standards of personal conduct

c. Are encouraged to include comments on performance ratings pertaining to application of security standards of conduct and discharge of security functions on all incumbents of positions designated as sensitive but not requiring access to classified information (i.e., performance of ADP sensitive functions).

## Section II

### Security Education

9-4. Security education briefing. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under AR 380-67 will be given an initial briefing and refresher briefings on an annual basis. The briefing will be conducted in accordance with AR 380-5, chapter X and consist of the elements noted in AR 380-67, paragraph 9-201. If the person is cleared for access to classified information, he should be informed of the degree of security clearance which was granted by CDR, CCF and the level of access required to perform his assigned duties. A record of these briefings will be maintained by the S2/security manager. Item 13, USAARMC Form 1378 should be used to record the initial briefing.

9-5. Nondisclosure Agreement (NDA). In accordance with AR 380-5, chapter 10-102, personnel granted a security clearance shall not be permitted to have access to classified information until they have signed Standard Form 312, Classified Information Nondisclosure Agreement. Implementing instructions for the NDA are contained in DA Circular 380-93-1. If the person declines to execute the NDA, action must be taken to informally suspend the individual's access to classified information for a 10 day period, allowing the individual time to reconsider signing the NDA. If at the end of the ten day period, the individual still declines to sign the NDA, the individual's access to classified information will be formally suspended and a DA Form 5248-R submitted. Item 11b, DA Form 5248-R must reflect the subject was given a ten day period to reconsider signing the NDA. The date the NDA was executed should be reflected in item 13, USAARMC Form 1378.

9-6. Foreign travel briefing. AR 380-67, paragraph 9-203a requires all personnel possessing a security clearance to report all foreign travel in advance of the travel being performed. This requirement has been modified as indicated below due to elimination of "designated countries" by OSD. These changes will appear in the revision of AR 380-67.

a. All cleared personnel (military, DA civilian, contractor) holding a TOP SECRET security clearance or having access to Sensitive Compartmented Information (SCI) will report all personal, unofficial foreign travel to their security manager in advance of the travel being performed. Travel by such personnel to contiguous countries may be reported after-the-fact; for example, Mexico and Canada for personnel stationed in CONUS; France and Luxembourg, Austria, Belgium, Netherlands, and Denmark for personnel stationed in Germany, etc.

b. Those persons who are cleared at the SECRET and CONFIDENTIAL level do not have to report personal foreign travel.

c. In addition to reporting data listed in AR 380-67, paragraph 9-203d individuals required to report personal foreign travel will also report mode of travel, contact persons at destination(s) and foreign addresses and telephone numbers if available. TRADOC Form 227-R is to be used in recording foreign travel. A copy of the form is provided at appendix W.

d. AR 25-400-2, The Modern Army Recordkeeping System (MARKS), does not contain a file number for personal foreign travel. Pending official publication in MARKS the following file number has been approved for use:

File Number: 380-67d  
 File Title: Personal Foreign Travel Records  
 Authority:  
 Privacy Act: A0380-67DAMI  
 Description: Information pertaining to personal foreign travel of individuals possessing DOD security clearances. Included are records of personal foreign travel, to include foreign travel briefings and debriefings.

Disposition: Retain in CFA until disposition instructions are published in AR 25-400-2.

e. Personnel with TOP SECRET access will be advised at the time of their initial briefing and at subsequent refresher briefings of the applicable reporting requirements for personal foreign travel. A foreign travel briefing will be given before official OCONUS travel. Assistance in preparation of your foreign travel briefings can be obtained by contacting the Information Security/Disclosure Branch, G3/DPTM, 4-7186/7172/2552.

9-7. Termination briefing.

a. Security managers are responsible to debrief personnel per AR 380-67, paragraph 9-204. DA Form 2962 (Security Termination Statement and Debriefing Certificate) or Standard Form 312 (Classified Information Nondisclosure Agreement) will be used for this purpose. The execution of SF 312 for departing personnel will be processed as described in DA Circular 380-93-1, chapter 4. A sample copy of a completed DA Form 2962 is provided at appendix X.

b. DA has expressed concern in the execution of security termination briefings to outgoing personnel, particularly, general officers and members of the Senior Executive Service. Your debriefing program must be designed in such a way to ensure all personnel, regardless of grade, receive appropriate debriefings. The debriefing should include reminders that the obligation to protect classified information, including that stored in one's memory, does not end with a person's departure from service/employment. A person who no longer has a security clearance is still subject to criminal and civil liability for the unauthorized disclosure of classified information accessed while cleared.

c. The DA Form 2962 or SF 312 must be retained for a minimum of 2 years after the individual is given a termination briefing. The individual should be provided a copy of the executed termination statement to show upon request when out processing the respective military or civilian personnel office.

see C1,  
12 Feb 98 9-8. \*

## Chapter 10

Safeguarding Personnel Security  
Investigative Records

10-1. General. Regulatory guidance for the safeguarding of personnel security investigative records is contained in AR 380-67, chapter 10.

10-2. Access to personal information contained in personnel security investigative reports and records should be handled with the highest degree of discretion and shall be afforded only for the purpose cited in AR 380-67. Primary rules to follow are:

a. Restrict access to information contained in investigative dossiers to those personnel in your activity who have an absolute need for access in connection with authorized personnel security actions.

b. Maintain the dossiers in the security office using a proper security container. Do not, repeat, do not put dossier material in an individual's personnel file.

c. Destroy the dossiers as soon as reasonable after you complete the associated personnel security action. AR 380-67 requires that they be destroyed within 90 days of completion. You may not maintain them past that point. Destruction shall be accomplished in the same manner as for classified information in accordance with AR 380-5.

d. Do not allow the subject or anyone representing subject access to the dossiers. If subject wants or needs information from the files, they must submit a request in accordance with the Privacy Act/Freedom of Information Act (see appendix Y, this pamphlet).

e. If you are going to use information from the dossiers for an unfavorable personnel action, you may extract information from them; however, you must be very careful when doing this. In particular, you may NOT use copies of actual material from the dossiers without the permission of the files holding agency. Rather, you must extract the information and put it in some other type of document. When you do this, do not reveal sources or information that could identify sources. Because of the sensitivity of this process, contact the Personnel Security Branch, Security Division, G3/DPTM whenever you are contemplating using dossier information in an unfavorable personnel proceeding.

10-3. Requesting/Reviewing Investigative Dossiers.

a. The only activities within the U.S. Army Armor Center authorized to request and store personnel security investigative dossiers are Security Division, G3/DPTM, and Trainee/Student Processing Division, G1/AG. Trainee/Student Processing Division is only authorized to request and store investigative files pertaining to trainees. Any personnel security investigative reports received by any other activity should be forwarded to Security Division in accordance with procedures outlined in AR 380-67, paragraph 10-103d.

b. If a commander or security manager requires an individual's dossier to determine the reason for a previous denial or revocation action, or to determine PRP eligibility, the security manager should submit a request for the individual's dossier to Security Division, G3/DPTM via memorandum. Memorandum must include subject's name, date of birth, state or country of birth, social security number and justification.

c. A list of personnel authorized to review investigative reports on file within Security Division will be submitted by the commander/director, if other than the designated security manager will be conducting the review. Appointment for review of file can be scheduled by contacting Personnel Security Branch, 4-1655/6741.

10-4. Disposition of Other Personnel Security Actions. Personnel security actions shall be destroyed 60 days after the subject has departed this installation. Actions pertaining to on-post transfers shall be forwarded to the gaining command security manager/S2.

FOR THE COMMANDER:



OFFICIAL:  
JACK L. SKIDMORE  
Colonel, GS  
Chief of Staff

ROBERT L. BROOKS  
Director, Information Management

DISTRIBUTION:  
B plus  
50 - ATZK-PTF-P

CF:  
DCG, USAARMC

Appendix A  
Superseded Documents

This pamphlet supersedes below listed documents:

a. Office Vision/PROFS note, E. MARIA LANE, subject: Personnel Security Update, dated:

- (1) 3 May 1994.
- (2) 7 January 1994.
- (3) 13 October 1993.
- (4) 3 May 1993.
- (5) 26 March 1993.

b. Memorandum, ATZK-PTF, 2 September 1993, subject: Personnel Security Update 3/93.

c. Memorandum, ATZK-DSP, subject: Personnel Security Update, dated:

- (1) 4 May 1992.
- (2) 3 March 1992.
- (3) 27 November 1991.
- (4) 1 July 1991.
- (5) 11 March 1991.
- (6) 5 September 1990.
- (7) 11 April 1990.
- (8) 14 December 1989.
- (9) 10 August 1989.

c. Memorandum, ATZK-DSP, 3 April 1992, subject: Reporting of Derogatory Information and Suspension of Access.

d. Memorandum, ATZK-DS, 23 January 1991, subject: Reunification of Germany.

C1, USAARMC Pam 380-67 (12 Feb 98)

e. Memorandum, ATZK-DSP, 3 August 1990, subject: Safeguarding Personnel Security Investigative Reports and Records.

f. Memorandum, ATZK-DS-PSD, 24 May 1988, subject: Implementing Instructions for Designation of ADP Sensitive Positions and Placement of Personnel in ADP Sensitive Positions.

g. Memorandum, ATZK-DS, 12 June 1987, subject: Intelligence Newsletter 87-3: Designation and Fill of Sensitive Positions.

h. Intelligence Newsletter 87-1, ATZK-DS, 20 February 1987, subject: Policy for Honoring an Existing Certificate of Clearance.

i. Intelligence Newsletter 85-2, ATZK-DS, 24 June 1985, subject: Personnel Security.

j. Letter, ATZK-DS, 1 September 1982, subject: Intelligence Newsletter 7-82.

l. Office Vision/PROFS note, subject: Interim change to USAARMC Pamphlet 380-67, 21 October 1994:

- (1) Interim Change 1
- (2) Interim Change 2
- (3) Interim Change 3
- (4) Interim Change 4
- (5) Interim Change 5
- (6) Interim Change 6
- (7) Interim Change 7
- (7a) Interim Change 7a
- (8) Interim Change 8
- (9) Interim Change 9

m. Office Vision/PROFS note, subject: Personnel Security Update:

- (1) Update 3-94

- (2) Update 4-94
- (3) Update 1-95
- (4) Update 2-95
- (5) Update 3-5
- (6) Update 4-95
- (7) Update 5-95
- (8) Update 6-95
- (9) Update 96-1
- (10) Update 96-2
- (11) Update 96-3
- (12) Update 96-4
- (13) Update 96-5
- (14) Update 96-6
- (15) Update 96-7
- (16) Update 97-1

Appendix B  
Responsible Commanders/Partners in Excellence

Commanders/Directors responsible for implementing personnel security provisions of this pamphlet are as follows:

- a. Commander, 1st Armor Training Brigade.
- b. Commander, 16th Cavalry Regiment.
- c. Commander, 3d Recruiting Brigade.
- d. Commander, U.S. Army NCO Academy.
- e. Commander, 703rd Explosive Ordnance Detachment.
- f. Commander, 280th MP Detachment.
- g. Commander, U.S. Army Medical Department Activities - Fort Knox.
- h. Commander, 731st Explosive Ordnance Detachment, Wright Patterson, AFB, Ohio.
- i. Commander, Readiness Group Harrison, Indianapolis, IN.
- j. Commander, 280th Military Police Detachment, (CID), 3d MI Group.
- k. Chief, U.S. Army Research Institute Armored Forces Research Unit.
- l. Director, U.S. Army Operational Test & Evaluation Command Test & Evaluation Coordination Office (Fort Knox).
- m. Chief, U.S. Army TMDE Support Center.
- n. Chief, AMC Logistic Assistance Office - Fort Knox.
- o. Commander, B Company 2/228 Aviation Flight Detachment.
- p. Commander, TRADOC Region D, Regional Element.

## Appendix C

## Items to Include in Supplemental Personnel Security Procedures

A comprehensive Personnel Security SOP must be developed which includes, but is not limited to, those items listed below. Issues which must be addressed in your SOP are those which subordinate elements need to be knowledgeable of.

- a. Areas of responsibility should be defined.
  - (1) Commander.
  - (2) Supervisor.
  - (3) Individual.
  - (4) Co-worker.
- b. In and out processing of assigned personnel.
- c. How to obtain a security clearance/special access.
- d. How to report unfavorable information. What to report, where to report, and how to report it.
- e. Commander's options pertaining to suspension/revocation actions.
- f. Designation of sensitive positions regarding military and civilian positions.
- g. Access rosters/USAARMC Form 1378.
  - (1) Preparation.
  - (2) Maintenance.
  - (3) Disposition.
- h. Security Education.
  - (1) Initial briefing.
  - (2) Refresher briefing.
  - (3) Debriefing.
- i. Foreign Travel.

- (1) Records of personal travel.
- (2) Briefings.
- (3) Debriefings.

j. Preparation of letters of recommendation as to whether the subject should or should not be granted a security clearance.

## INSPECTION CHECKLIST

<b>FUNCTIONAL AREA:</b> Security	<b>SUBJECT AREA:</b> Personnel Security Program	<b>PAGE 1</b> of 6 PAGES
<b>PROPONENT/PHONE NO:</b> Security Division, G3/DPTM, 4-1655/7111		<b>DATE OF REVISION:</b> 26 Apr 96
<b>UNIT INSPECTED:</b>	<b>DATE:</b>	<b>INSPECTOR'S NAME/PHONE NO:</b>

YES	NO	NA	
			<p><b>REFERENCES:</b></p> <p>AR 380-67, 9 September 1988, Personnel Security Program.</p> <p style="margin-left: 20px;">a. USAARMC Pamphlet 380-67, 21 October 1994, Personnel Security Program</p> <p style="margin-left: 20px;">b. Personnel Security Updates.</p> <p><b>PROGRAM MANAGEMENT:</b></p> <p>1. Has an official been appointed to serve as security manager/alternate (USAARMC Pamphlet 380-67, paragraph 3-1)?</p> <p>2. Have comprehensive supplemental personnel security procedures been developed which comply with USAARMC Pamphlet 380-67, paragraph 3-2 and appendix C?</p> <p>3. Has a program been established for self-inspection and periodic oversight inspections of subordinate elements (AR 380-67, paragraph 11-101h(7) and USAARMC Pamphlet 380-67, paragraph 2-4d)?</p> <p style="margin-left: 20px;">a. Are the inspections conducted as a minimum once every 2 years?</p> <p style="margin-left: 20px;">b. Are inspection results placed in writing and available for review?</p> <p>4. Are supplemental questionnaires/checklists being used as an evaluation procedure in support of the Personnel Security Program (USAARMC Pamphlet 380-67, paragraph 3-12)?</p> <p>5. Are S2 personnel/security managers thoroughly familiar with pertinent regulations and the responsibilities of their positions (USAARMC Pamphlet 380-67, paragraph 2-4b)?</p> <p><b>DESIGNATION OF SENSITIVE POSITIONS:</b></p> <p>1. Have all civilian positions within the activity been categorized as either nonsensitive, noncritical-sensitive or critical-sensitive (AR 380-67, paragraph 3-101 and USAARMC Pamphlet 380-67, paragraph 4-2)?</p> <p style="margin-left: 20px;">a. Have the sensitive positions been approved by CDR/Director of your activity, (USAARMC Pamphlet 380-67, paragraph 4-3)?</p> <p style="margin-left: 20px;">b. Are approved copies of the SF 52 on file within the activity (USAARMC Pamphlet 380-67, paragraph 4-4b)?</p>

<b>INSPECTION CHECKLIST (continued)</b>			
<b>FUNCTIONAL AREA:</b> SECURITY		<b>SUBJECT AREA:</b> PERSONNEL SECURITY	
		PAGE 2 of 6 PAGES	
YES	NO	NA	
			<p>c. Are all changes affecting a sensitive position reported to Security Division, G3/DPTM as they occur (USAARMC Pamphlet 380-67, paragraph 4-4c)?</p> <p>d. Are personnel occupying sensitive positions properly cleared or an exception to policy granted before hire (AR 380-67, paragraph 3-204 and USAARMC Pamphlet 380-67, paragraph 4-8)?</p> <p>2. Have military personnel security requirements been identified in SIDPERS Authorized Strength Files(SASF) (DA Pam 600-8 and USAARMC Pamphlet 380-67, paragraph 4-9)?</p> <p><b>INITIATION OF PERSONNEL SECURITY ACTIONS:</b></p> <p>1. Are the number of persons cleared for access to classified information kept to a minimum consistence with the requirements of operations or MOS/occupational skills (AR 380-67, paragraph 2-501 and USAARMC Pamphlet 380-67, paragraph 3-4)?</p> <p>2. Are requests for clearance/investigations canceled when no longer needed (AR 380-67, appendix C-1e, AR 380-67 and USAARMC Pamphlet 380-67, paragraph 3-5)?</p> <p>3. Are request for interim security clearance kept to a minimum (AR 380-67, paragraph 5-104 and USAARMC Pamphlet 380-67, paragraph 6-5)?</p> <p>4. Is proper planning exercised to ensure that personnel security investigations are submitted sufficiently in advance to allow completion of the investigation prior to the time it is needed to grant the required clearance or make the necessary personnel security determination (AR 380-67, paragraph 5-100 and USAARMC Pamphlet 380-67, paragraph 5-1)?</p> <p style="padding-left: 20px;">a. Does the activity have a functional suspense management program?</p> <p style="padding-left: 20px;">b. Are request for local file checks initiated immediately and follow-up actions exercised to ensure they are received in a timely fashion?</p> <p style="padding-left: 20px;">c. Is subject notified immediately of required forms to be completed and its urgency stressed as to expeditious completion of said forms?</p> <p style="padding-left: 20px;">d. Have "Catch Em In CONUS" program procedures been established (USAARMC Pamphlet 380-67, Section IV, Chapter 5.</p> <p style="padding-left: 20px;">e. Are required forms and prescribed documentation properly executed (USAARMC Pamphlet 380-67, paragraph 5-2)?</p> <p>5. Have all personnel engaged in education and orientation duties had a favorable NAC (AR 380-67, paragraph 3-611)?</p> <p>6. Are incumbents of critical-sensitive and noncritical sensitive-SECRET positions required a to undergo a PR every 5 and 15 years, respectively (AR 380-67, paragraph 3-703 and USAARMC Pamphlet 380-67, paragraphs 5-10 and 5-11)?</p>

## INSPECTION CHECKLIST CONTINUATION SHEET

FUNCTIONAL AREA:  
SECURITY

SUBJECT AREA:  
PERSONNEL SECURITY

PAGE 3  
of 6 PAGES

YES	NO	NA	
			<p>7. Is access being suspended and DA Form 5248-R forwarded to CCF on individuals failing to complete the required PR within the time prescribed or refusing to complete the forms (AR 380-67, paragraph 5-105c and USAARMC Pamphlet 380-67, paragraph 5-13)?</p> <p>8. Is U.S. Citizenship verification being completed?</p> <p style="padding-left: 20px;">a. Is citizenship verification accomplished by a commissioned or warrant officer, noncommissioned officer in grade E-7 or above or DA civilian GS07 or above (USAARMC Pamphlet 380-67, paragraph 3-10b)?</p> <p style="padding-left: 20px;">b. Are personnel verifying citizenship adequately trained in the review of citizenship documentation (USAARMC Pamphlet 380-67, paragraph 3-10b)?</p> <p style="padding-left: 20px;">c. Are double check procedures implemented to confirm a soldier or civilian is beyond reasonable doubt a U.S. citizen (USAARMC Pamphlet 380-67, paragraph 3-10c)?</p> <p style="padding-left: 20px;">d. Are records maintained which specify who and what document was used to verify an individual's U.S. citizenship (USAARMC Pamphlet 380-67, paragraph 3-10d)?</p> <p style="padding-left: 20px;">e. Have procedures been established to ensure security clearances previously issued to immigrant aliens are reissued as Limited Access Authorizations or administratively withdrawn (AR 380-67, paragraphs 2-100 and 3-403)?</p> <p>10. Is subject's federal service date without a 24 month break as defined in AR 380-67, paragraph 1-306.1 verified through official means (USAARMC Pamphlet 380-67, paragraph 3-7a (1))?</p> <p>11. Are unit S2s/security managers ensuring local files checks are not over 60 days old before submission of personnel security actions (USAARMC Pamphlet 380-67, paragraph 3-7a)?</p> <p>12. Are local file checks being properly completed to include unit files for pending unit punishment, records, of indebtedness, etc. (USAARMC Pamphlet 380-67, paragraph 3-7a (4))?</p> <p>13. Are DA Forms 873 being removed from MPRJ/OPF under conditions other than cited in AR 380-67, paragraphs 8-102 and 8-201)?</p> <p><b>GRANTING ACCESS</b></p> <p>1. Is access to classified information granted only to persons whose official duties require such access and who have the appropriate personnel security clearance validated by the local command (AR 380-67, paragraph 7-102, and USAARMC Pamphlet 380-67, paragraph 6-9)?</p> <p>2. Is access eligibility being withdrawn when no longer required in the normal course of an individual's duties (AR 380-67, paragraph 7-4)?</p>

<b>INSPECTION CHECKLIST CONTINUATION SHEET</b>			
FUNCTIONAL AREA: <b>SECURITY</b>		SUBJECT AREA: <b>PERSONNEL SECURITY</b>	
		PAGE <b>4</b>	of 6 <b>PAGES</b>
YES	NO	NA	
			<p>3. Is an individual's access downgraded when the security clearance is based on an outdated investigation and a request for a periodic reinvestigation was not forwarded within the specified time frame (AR 380-67, paragraph 7-103 and USAARMC Pamphlet 380-67, paragraph 5-12)?</p> <p>4. Are USAARMC Forms 1378 utilized for accepting security clearance/surety determinations on assigned or attached personnel (USAARMC Pamphlet 380-67, paragraph 6-10)</p> <p style="margin-left: 20px;">a. Is the degree of clearance/date and type/date of investigation being properly extracted from the DA Form 873?</p> <p style="margin-left: 20px;">b. Are local files checks being completed and appropriate annotations made on the form?</p> <p style="margin-left: 20px;">c. Is the individual signing the USAARMC Form 1378 the security manager or intelligence officer?</p> <p style="margin-left: 20px;">d. Do the USAARMC Forms 1378 reflect current clearance/investigation status?</p> <p>5. Are previously granted clearances only being accepted when they are computer generated by CCF, local file checks are favorable and there has been no break in Federal service exceeding 24 months since the investigation date (AR 380-67, paragraph 7-102, and USAARMC Pamphlet 380-67, paragraph 6-9a)?</p> <p>6. Is local access authorized military personnel recorded in the SIDPERS Personnel File (SPF), Field Determined Personnel Security Status (DA Pam 600-8, paragraph 9-30; DA Pam 600-8-1 and USAARMC Pamphlet 380-67, paragraph 6-10a)?</p> <p>7. Is security clearance indicated on TDY orders only after written verification is received from the security manager (USAARMC Pamphlet 380-67, paragraph 6-12)?</p> <p><b>REPORTING OF UNFAVORABLE INFORMATION</b></p> <p>1. Is all significant unfavorable information pertaining to assigned or attached personnel being reported on DA Form 5248-R (AR 380-67, paragraph 8-101 and USAARMC Pamphlet 380-67, paragraphs 8-2 and 8-5)?</p> <p style="margin-left: 20px;">a. Are DA Forms 5248-R being properly completed? Is all amplifying information being provided to enable an adjudicator to make a thorough and comprehensive security evaluation?</p> <p style="margin-left: 20px;">b. Are follow-up reports forwarded within 60 days (USAARMC Pamphlet 380-67, paragraph 8-5b)?</p> <p style="margin-left: 20px;">c. Do final reports contain recommendations of the command concerning restoration of the person's access or revocation of their security clearance (AR 380-67, paragraph 8-101 and USAARMC Pamphlet 380-67, appendix T, item 12c)?</p> <p style="margin-left: 20px;">d. Is the subject notified in writing when access to classified information/SCI has been suspended (USAARMC Pamphlet 380-67, paragraph 8-13a)?</p>

## INSPECTION CHECKLIST CONTINUATION SHEET

FUNCTIONAL AREA:  
SECURITY

SUBJECT AREA:  
PERSONNEL SECURITY

PAGE 5  
of 6 PAGES

YES	NO	NA

2. Is the commander/supervisor knowledgeable of the responsibility to report all credible derogatory information on assigned personnel and options concerning suspension action when the information falls within the scope of AR 380-67, paragraph 2-200 and the individual has a security clearance (AR 380-67, paragraphs 8-101 and 8-102, and USAARMC Pamphlet 380-67, paragraphs 8-2 and 8-12)?

a. Are S2 personnel assisting the command by coordinating with legal clerk for actions such as Article 15, court-martials, suspension of favorable personnel actions, discharge packets, etc.?

b. Are S2 personnel coordinating with unit drug/alcohol representative when information is required on drug/alcohol program enrollment/status?

3. Is an individual's name deleted from all access rosters or appropriate SIDPERS transaction made when notified of suspension/revocation action (USAARMC Pamphlet 380-67, paragraph 8-13b)?

**CONTINUING SECURITY RESPONSIBILITIES:**

1. Is the individual concerned informed when granted a security clearance as to the degree of clearance and responsibility to protect classified information and the adverse effects to national security resulting from compromise (AR 380-67, paragraphs 9-200 and 9-201, and USAARMC Pamphlet 380-67, paragraph 9-4)?

2. Are commanders/supervisors familiar with their responsibilities in matters pertaining to personnel security with respect to personnel under their supervision (AR 380-67, paragraph 9-102 and USAARMC Pamphlet 380-67, paragraph 9-1)?

3. Is a comment regarding an employee's discharge of security responsibilities being made in conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information (AR 380-67, paragraph 9-102d and USAARMC Pamphlet 380-67, paragraph 9-3b)?

4. Is special counseling made available to encourage individuals cleared under AR 380-67 to seek appropriate guidance on any personal problem or situation that may have a bearing on their eligibility to remain in a position of trust (AR 380-67, paragraph 9-101, and USAARMC Pamphlet 380-67, paragraph 9-3)?

5. Are personnel holding a TOP SECRET security clearance knowledgeable of the requirement to report all personal foreign travel in advance of the travel being performed (AR 380-67, paragraph 9-203 and USAARMC Pamphlet 380-67, paragraph 9-6a)?

a. Is TRADOC Form 227-R being used to record foreign travel (USAARMC Pamphlet 380-67, paragraph 9-6c)?

b. Is information pertaining to personal foreign travel forwarded to the gaining command upon transfer of the individual (AR 380-67, paragraph 9-203)?

c. Is a copy of TRADOC Form 227-R retained for 1 year after PCS or for 5 years after retirement, separation, or termination of employment of the individual (AR 380-67, paragraph 9-203d)?

<b>INSPECTION CHECKLIST CONTINUATION SHEET</b>			
FUNCTIONAL AREA: <b>SECURITY</b>		SUBJECT AREA: <b>PERSONNEL SECURITY</b>	
		PAGE <b>6</b>	of 6 PAGES
YES	NO	NA	
			<p>6. Are termination briefings given to employees 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. (AR 380-67, paragraph 9-204)?</p> <p style="padding-left: 20px;">a. Execute a Security Termination Briefing DA Form 2962 or the back side of the SF 312 for individuals retiring, ETS'ing, resigning from civilian service, revocation of a security clearance or contemplated absence from duty or employment for 60 days or more. (AR 380-67, paragraph 9-204 and USAARMC Pamphlet, paragraph 9-7)?</p> <p><b>SAFEGUARDING PERSONNEL SECURITY REPORTS AND RECORDS</b></p> <p>1. Are personnel security actions stored in a locked container or in a similar protected area (AR 380-67, paragraph 10-103 and USAARMC Pamphlet 380-67, paragraph 10-2b)?</p> <p>2. Is an individual's status with respect to a personnel security clearance or a special access authorization protected and only released based on an established need-to-know basis (AR 380-67, paragraph 10-103e)?</p> <p>3. Is proper disposition made of investigative files and other personnel security actions upon transfer or separation of the individual from the activity (AR 380-67, paragraph 10-104 and USAARMC Pamphlet 380-67, paragraphs 10-2c and 10-4)?</p> <p>4. Are personnel security reports and records afforded only for the purpose cited in AR 380-67, chapter 10, and to persons whose official duties require such information (AR 380-67, paragraph 10-100 and USAARMC Pamphlet 380-67, paragraph 10-2)?</p> <p>5. Are investigative dossiers received through the mail forwarded to Security Division, G3/DPTM for storage (USAARMC Pamphlet 380-67, paragraph 10-3)?</p>

Appendix E

Security Clearance Requirements for MOS, MOS-Producing Schools, Functional Areas, and Additional Skill Identifiers

E-1. Enlisted MOS and MOS-producing schools (reference AR 611-201, 26 June 1995, Enlisted Career Management Fields and Military Occupational Specialty, and DA Pamphlet 351-4, 31 October 1995, U.S. Army Formal Schools Catalog, DA Circular 611-96-1, 25 October 1996, Implementation of Changes to the Military Occupational Classification and Structure).

13C - *SECRET	27M - *SECRET	52E - SECRET
13E - SECRET	27T - *CONF	55B - SECRET
13F - CONF	27X - *SECRET	55D*SECRET/SSBI/PRP
13M - SECRET	27Z - SECRET	68N- SECRET (*CONF)
13P - *SECRET	31C -SECRET (*CONF)	68P - SECRET
13R - *SECRET	31F - SECRET	68R - *SECRET
13Z - SECRET	31L - SECRET	71C - SECRET
14D - *SECRET	31P - *SECRET	74B - SECRET/PSSP
14E - *SECRET	31R - SECRET	74C - **TS/SCI
14J - *SECRET	31S - *SECRET	74G-TS/SCI (*SECRET)
14L - *SECRET	31T - SECRET	74Z - SECRET
14M - *SECRET	31U - SECRET	75F - SECRET
14R - *SECRET	31W - SECRET	81T - SECRET
14S - *SECRET	31Z - SECRET	93B - SECRET
14T - *SECRET	33R - ***TS/SCI	93P - SECRET
14Z - *SECRET	33T - ***TS/SCI	95B - CONF/PRP
16P - *SECRET	33Y - ***TS/SCI	96B - ***TS/SCI
16S - *SECRET	33Z - ***TS/SCI	96D - ***TS/SCI
16T - *SECRET	35B - SECRET	96H - *SECRET
16Z - *SECRET	35C - SECRET	96R - *SECRET
18B - *SECRET	35E - *SECRET	96U - *SECRET
18C - *SECRET	35F - SECRET	96Z - TS/SCI
18D - *SECRET	35J - SECRET	97B - ***TS/SCI
18E - *SECRET	35M - SECRET	97E - SECRET
18F - SECRET	35N - SECRET	97G - ***TS/SCI
18Z - SECRET	35W - SECRET	97L - SECRET
23R - *SECRET	35Y -SECRET (*CONF)	97Z - TS/SCI
24H - CONF	35Z - *SECRET	98C - ***TS/SCI
24K - CONF	37F - *SECRET	98D - ***TS/SCI
24N - *SECRET	38A - *SECRET	98G - ***TS/SCI
27E - *SECRET	39B - *SECRET	98H - ***TS/SCI
27G - *SECRET	45G - *CONF	98J - ***TS/SCI
27H - *SECRET	45K - CONF	98K - ***TS/SCI
27K - *SECRET		98Z - TS/SCI

C1, USAARMC Pam 380-67 (12 Feb 98)

E-2. Warrant Officer MOS (reference AR 611-112, 26 June 1995, Manual of Warrant Officer Military Occupational Specialties). A minimum of an Interim SECRET is required to apply for warrant officer. A final clearance must be granted prior to the individual attending the warrant officer school.

311A - TS/SSBI	351C - TS/SCI	352H - TS/SCI
350B - TS/SCI	351E - TS/SCI	352J - TS/SCI
350D - TS/SCI	352C - TS/SCI	352K - TS/SCI
350L - TS/SCI	352D - TS/SCI	353A - TS/SCI
351B - TS/SCI	352G - TS/SCI	910A - SECRET/PRP

E-3. Commissioned Officer (references AR 611-101, 26 June 1995, Commissioned Officer Classification System, DA Pamphlet 600-3, 8 Jun 1995, Commissioned Officer Development and Career Management). A minimum of final SECRET is required before to being commissioned and applying for Officers Candidate School (OCS).

a. Functional area.

Aviation Tactical Intelligence (15) - TS/SCI

Special Forces (18) - Eligible for TS

Military Intelligence (35) - TS/SCI

Foreign Area Officer (48) - TS/SCI

b. Additional skill identifier 3E - TS/SCI.

\* Indicates clearance required to attend MOS-producing course. Interim clearances authorized.

\*\* Reserve/National Guard require a SECRET clearance.

\*\*\* Interim authorization for TS/SCI (Open SSBI at DIS and favorable adjudication of NAC or ENTNAC by CCF prior to ship)

F-2. Location/Address to Conduct/Obtain Records Check.

a. Personnel Records (MPRJ/OPF RCDS)

(1) Military (less trainees) - ATZK-AGS, Bldg 5101

Trainees - ATZK-AGT, Bldg 6590

(2) DA Civilian - ATZK-HRC-E, Bldg 2197

b. Medical Records (MED RCDS)

(1) Military

MCXM-AMC (Gold Clinic)	MCXM-AMJ (Red Clinic)	MCXM-AMV (Blue Clinic)
HHC 1ATB	16th Cav Reg	USAREC
2/13 Bn	MEDDAC	USAARMC
5/15 Cav	DENTAC	2nd Region ROTC Cadet
1/81 Bn	VET Activity	LEC
3/81 Bn	NCOA	Readiness Tng Bde
1/46 Inf Bn		Readiness Gp Knx
2/46 Inf Bn		Knox Tng Gp
46th AG		DFAS
		113th Army Band
		121 ARCOM
		71DD Det
		Blue Grass Depot
		OPTIC TECO Ft Knox

(2) DA Civilians MCXM-PAR, Bldg 851

c. Provost Marshal Records (PMO RCDS) - ATZK-PM-R Bldg 204

d. Intelligence Records (INTEL RCDS) - ATZK-PTF-P, Bldg 1109A

e. Unit Records (Unit RCDS)- Unit Commander (not required for civilians).

f. Finance Records (NOT REQUIRED)

**INDIVIDUAL FINANCIAL STATEMENT**

NAME: \_\_\_\_\_ SSN: \_\_\_\_\_ DATE: \_\_\_\_\_

**MONTHLY INCOME**

Gross Salary \$ \_\_\_\_\_  
 - Total Deductions \$ \_\_\_\_\_  
 Net Salary (Take-home pay) \$ \_\_\_\_\_  
 Spouse's Net Salary \$ \_\_\_\_\_  
 Other Income (Explain source in remarks section) \$ \_\_\_\_\_

**TOTAL NET MONTHLY INCOME** \$ \_\_\_\_\_

**MONTHLY EXPENSES**

Rent (List mortgage below) \$ \_\_\_\_\_  
 Groceries \$ \_\_\_\_\_  
 Clothing \$ \_\_\_\_\_  
 Utilities (gas, electric, water, telephone, trash, etc.) \$ \_\_\_\_\_  
 Car Expense (insurance, repairs, gasoline, etc.) \$ \_\_\_\_\_  
 Life/Other Insurance \$ \_\_\_\_\_  
 Medical Expense \$ \_\_\_\_\_  
 Alimony/Child Support/Day Care \$ \_\_\_\_\_  
 Miscellaneous (entertainment, transportation, etc.) \$ \_\_\_\_\_

**TOTAL MONTHLY EXPENSES** - \$ \_\_\_\_\_

**DEBTS**

LIST ALL FINANCIAL OBLIGATIONS BY  
 NAME OF PERSON/COMPANY/FIRM

	TOTAL AMT OWED	DATE OF LAST PMT	AMT OF MO PMT
Mortgage: _____	\$ _____	_____	\$ _____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

(Continue list on separate sheet if necessary.)

INCLUDE ALL PAYMENTS IN THIS TOTAL →

**TOTAL ACTUAL MONTHLY PAYMENTS** - \$ \_\_\_\_\_

**NET REMAINDER AFTER EXPENSES AND DEBT PAYMENT** = \$ \_\_\_\_\_

**REMARKS:**