

Headquarters
US Army Garrison Command
Fort Knox, Kentucky 40121-5721
24 July 2008

*Fort Knox Pam 380-67

Security

PERSONNEL SECURITY PROGRAM

Summary. This pamphlet contains policy guidance disseminated by Army Regulation (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 AR 380-67, The Department of the Army 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 regulation is the Security Division, Directorate of Plans, Training, Mobilization, and Security (DPTMS). Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Security Division, DPTMS (IMSE-KNX-PLSP), Fort Knox, Kentucky 40121-5721.

Table of Contents

	Paragraph	Page
Chapter 1 – General Provisions		
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		
Section I – General	2-1	2-1
Section II – Responsibilities		
Security Division	2-2	2-1
Civilian Personnel Advisory Center (CPAC)	2-3	2-1

*This pamphlet supersedes USAARMC Pam 380-67, 21 October 1994.

Table of Contents (Continued)

	Paragraph	Page
Commander	2-4	2-2
S2/Security Managers	2-5	2-2
Immediate Commanders/Supervisors	2-6	2-2
Individuals	2-7	2-3
Co-Workers	2-8	2-3
Inspections	2-9	2-3
Advice and Assistance Visits	2-10	2-4
 Chapter 3 – General Policy		
Appointment of Security Manager	3-1	3-1
Supplemental Personnel Security Standing Operating Procedures (SOP)	3-2	3-1
Routing of Personnel Security Actions	3-3	3-1
Limit Investigations and Security Clearances	3-4	3-1
Cancellations	3-5	3-1
Suspense Dates	3-6	3-1
Local Records Check (LRC)	3-7	3-2
Central Clearance Facility (CCF) Telephone Terminal	3-8	3-3
Citizenship	3-9	3-3
Designated Countries	3-10	3-4
Supplemental Questionnaires	3-11	3-4
Social Security Numbers Transmitted Over the Intranet	3-12	3-4
 Chapter 4 – Designation of Sensitive Positions		
Section I – General	4-1	4-1
Section II – Civilian Positions		
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	4-1
Position Sensitivity Roster	4-5	4-2
Investigative Requirements	4-6	4-2
Procedures for Filling a Position	4-7	4-2
Section III – Military Positions		
Personnel Security Requirements	4-8	4-3
 Chapter 5 – Requesting Personnel Security Investigations		
Section I - General		
Security Clearance Categories	5-1	5-1
Execution of the Investigation	5-2	5-1
Section II - Types of Investigation and Forms Required		
Entrance National Agency Check (ENTNAC)/National Agency Check (NAC)	5-3	5-1
National Agency Check (NAC)	5-4	5-2

Table of Contents (Continued)

	Paragraph	Page
National Agency Check, Local Agency Checks, and Credit Check (NACLC)	5-5	5-2
SECRET Periodic Reinvestigation (SECRET/PR)	5-6	5-2
National Agency Check with Written Inquiries (NACI)	5-7	5-3
Access National Agency with Written Inquiries (ANACI)	5-8	5-3
Single Scope Background Investigation (SSBI)	5-9	5-3
Periodic Reinvestigations (PRs)	5-10	5-4
Failure or Refusal to Complete a SECRET/PR or PR	5-11	5-4
Fingerprinting	5-12	5-4
Civilian Investigations Versus Military Investigations	5-13	5-4
Military Occupational Specialties (MOS) and Occupational Skills	5-14	5-5
 Chapter 6 – Requesting Security Clearance and Granting Access		
Section I - Requesting Security Clearance		
Granting Authority	6-1	6-1
Limitations	6-2	6-1
Limited Access Authorizations (LAA)	6-3	6-1
Interim Security Clearances	6-4	6-1
Personnel Security Actions for Reassignment	6-5	6-2
Promotions Based on Rank/MOS	6-6	6-2
Officers Security Requirement	6-7	6-2
Section II - Granting Access		
Accepting a Validated Clearance	6-8	6-2
Access Authorization/Documentation of Security Clearance Using FK Form 1378	6-9	6-3
Security Access Roster (SAR)	6-10	6-3
Verification of Security Clearance/Access Authorization for TDY Personnel	6-11	6-3
Visit Requests	6-12	6-3
 Chapter 7 – Special Access Programs		
Section I - Sensitive Compartmented Information (SCI)		
General	7-1	7-1
SCI Access	7-2	7-1
Investigative Requirement	7-3	7-1
Nomination Procedures	7-4	7-1
Transfer-In-Status	7-5	7-2
Indoctrination	7-6	7-2
Debriefing	7-7	7-3
Termination of Access	7-8	7-3
Section II - Nuclear Weapons Personnel Reliability Program (PRP)		
Governing Regulations	7-9	7-3

Table of Contents (Continued)

	Paragraph	Page
Investigative Requirements	7-10	7-3
Supplemental Guidance	7-11	7-3
Section III - Chemical Surety		
Governing Regulation	7-12	7-4
Investigative Requirements	7-13	7-4
Section IV - Information Systems Security		
Governing Regulations	7-14	7-4
Investigative Requirements	7-15	7-4
Network Access and Security Clearance Suspension/Denial/Revocation	7-16	7-4
Section V - Access to North Atlantic Treaty Organization (NATO)		
Classified Information		
Governing Regulations	7-17	7-5
Investigative Requirements	7-18	7-5
Section VI - Critical Nuclear Weapon Design Information (CNWDI)		
Governing Regulation	7-19	7-5
Briefing and Debriefing	7-20	7-5
Section VII - Special Access Program		
Governing Regulations	7-21	7-6
Chapter 8 – Unfavorable Administrative Actions		
Section I - Reporting of Unfavorable Information		
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
Alcohol Incident	8-6	8-2
Misuse of Government Travel Card	8-7	8-2
Misuse of Government computer	8-8	8-2
Unauthorized Absence or Suicide	8-9	8-3
Release of Information	8-10	8-3
Security Manager Responsibility	8-11	8-3
Section II - Suspension of Access		
Governing Regulation	8-12	8-3
Purpose of Suspension of Access	8-13	8-3
Formal/Informal Suspension	8-14	8-3
Guidance Upon Suspension of Access	8-15	8-4
Section III - Unfavorable Administrative Action Procedures		

Table of Contents (Continued)

	Paragraph	Page
Governing Regulation	8-16	8-4
Letters of Intent	8-17	8-4
Appeals and Reconsiderations	8-18	8-6
Security Manager's Responsibilities	8-19	8-6
Involuntary Separation	8-20	8-6
 Chapter 9 – Continuing Security Responsibilities		
Section I - Responsibilities		
Evaluating Continued Security Eligibility	9-1	9-1
Standards of Conduct	9-2	9-1
Commander/Supervisors	9-3	9-1
Section II - Security Education		
Security Education Briefing	9-4	9-1
Nondisclosure Agreement (NDA)	9-5	9-2
Foreign Travel	9-6	9-2
Termination Briefing	9-7	9-2
Change in Status of Individual	9-8	9-3
 Chapter 10 – Safeguarding Personnel Security Investigative Records		
General	10-1	10-1
Safeguarding the Information	10-2	10-1
Requesting/Reviewing Investigative Dossiers	10-3	10-1
Requesting Information Under Freedom of Information	10-4	10-2
Disposition of Other Personnel Security Actions	10-5	10-2
 Appendices		
A. Inspection Checklist		A-1
B. Items to Include in Supplemental Personnel Security Standing Operating Procedures		B-1
C. MOS Listing		C-1
D. FK Form 1947 (Local Files Check)		D-1
E. Acceptable Documents for Proof of U.S. Citizenship		E-1
F. Standard Subject Interview Worksheet		F-1
G. Designation of Sensitive Positions		G-1
Criteria for Position Sensitivity Designation	G-1	G-1
Criteria for IT Positions and Application	G-2	G-2
Detailed Instructions for Completing SF 52-B	G-3	G-3
Investigative Requirements	G-4	G-4
H. Request for Exception to Policy to Hire		H-1
Interim Clearance Required		H-1
No Interim Clearance Required		H-2
Previous Valid Clearance		H-3
Non-Critical Sensitive, No Clearance Required		H-4

Table of Contents (Continued)

	Paragraph	Page
I. Joint Personnel Adjudication System Instructions		I-1
J. Subjects e-QIP Quick Reference		J-1
K. Electronic Questionnaires for Investigations Processing (e-QIP)		K-1
Security Manager-s e-QIP Quick Reference	K-1	K-1
e-QIP/JAPAS Work-Arounds	K-2	K-3
How to Add a Record	K-3	K-4
L. Fingerprint		L-1
M. DA Form 5247-R, Request for Security Determination		M-1
N. Instructions for Completion of FK Form 1378		N-1
O. Security Access Roster		O-1
P. Nomination for Access to Sensitive Compartmented Information (SCI)		P-1
Q. Examples of Reportable Information (AR 380-67, Appendix I)		Q-1
R. DA Form 5248-R, Report of Unfavorable Information for Security Determination		R-1
S. Suspension of Access to Classified Information		S-1
Sample Memorandum for Suspension of Access to Classified Information		S-1
Sample Acknowledgement for Suspension of Access to Classified Information		S-2
T. Rebuttal Guidelines		T-1
U. Initial Security Briefing		U-1
V. DA Form 2962, Security Termination Statement		V-1

Chapter 1

General Provisions

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

1-2. Referenced Publications.

- a. AR 380-67, The Department of the Army Personnel Security Program, 9 September 1988.
- b. DA Pamphlet 600-8, Military Personnel Management, 1 October 1989.
- c. AR 380-5, Department of the Army Information Security Program, 29 September 2000.
- d. U.S. Office Of Personnel Management, Requesting OPM Personnel Investigations, May 2001.
- e. AR 50-6, Chemical Surety, 26 June 2001.
- f. AR 380-381, Special Access Programs (SAPS) and Sensitive Activities, 21 April 2004.
- g. AR 635-200, Active Duty Enlisted Administrative Separations, 6 June 2005.
- h. AR 600-85, Army Substance Abuse Program (ASAP), 24 March 2006.
- i. JAFAN 6/4, Joint Air Force-Army-Navy (JAFAN 6/4), 9 May 2006.
- j. DA Pamphlet 600-8-11, Reassignment, 1 May 2007.
- k. AR 601-210, Active and Reserve Components Enlistment Program, 7 June 2007.
- l. AR 25-2, Information Assurance, 24 October 2007.
- m. AR 600-8-19, Enlisted Promotions and Reductions, 20 March 2008.
- n. AR 40-66, Medical Record Administration and Health Care Documentation, 17 June 2008.

1-3. Referenced Forms.

- a. DA Form 2962 (Security Termination Statement).
- b. DD Form 1966/2 (Record of Military Processing - Armed Forces of the United States).
- c. Standard Form 312 (Classified Information Nondisclosure Agreement).

Fort Knox Pam 380-67 (24 Jul 08)

- d. Fort Knox Form 1378 (Record of Personnel Security Clearance/Action).
- e. Fort Knox Form 1947 (Local Files 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 Reserve Officers' Training Corps (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

Section I

General

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

Section II

Responsibilities

2-2. Security Division. The Chief, Security Division, has staff responsibility for providing guidance, oversight, and development of policy and procedures governing the personnel security program. The Chief, Personnel Security Branch, is functionally responsible for the administration of this program. Responsibilities include the following:

- a. Providing program management through issuance of local policy, operating guidance, and oversight.
- b. Providing staff assistance to commanders/directors/chiefs and security managers in resolving personnel security matters.
- c. Conducting inspections of service activities for implementation and compliance with pertinent personnel security regulations and directives.
- d. Maintaining rosters of civilian positions designated as sensitive, as well as a Security Access Roster of both military and civilian employees who have validated clearances within the activity.
- e. Granting interim security clearances and suspending access.
- f. Reviewing and processing requests for personnel security determinations.
- g. Approving requests for exception to policy for new hires before appointment to a sensitive position, assignment to sensitive duties, or access to classified information, pending completion of the required investigation.

2-3. Civilian Personnel Advisory Center (CPAC). The CPAC is responsible for the following:

- a. Ensuring that no individual occupies a noncritical-sensitive or critical-sensitive position until the appropriate investigative requirement is met.
- b. Initiating and monitoring all National Agency Checks with Written Inquiries (NACI) until completion.

c. Providing basic information to the Chief, Security Division, DTPMS, on derogatory cases that come to their attention.

2-4. Commander. Commanders, directors, or division chiefs are responsible for the following:

a. Implementing personnel security provisions of AR 380-67 and this pamphlet.

b. Appointing an individual, preferably the S2 or security manager, to perform personnel security functions.

2-5. S2/Security Managers. S2/Security Managers are responsible for performing personnel security functions, as outlined in AR 380-67 and this pamphlet. Specific functions include the following:

a. Initiating requests through the Joint Personnel Adjudication System (JPAS) for personnel security investigations.

b. Assisting personnel in reviewing SF 86 for errors in the Electronic Questionnaires for Investigative Processing (e-QIP).

c. Reporting adverse information.

d. Suspending an individual's access to classified information upon request.

e. Requesting security clearances.

f. Accepting previously granted security clearances.

g. Conducting oversight visits or inspections of subordinate activities at least once a year.

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

i. Maintaining a roster of civilian and military positions designated as sensitive.

j. Conducting initial, refresher, and termination security briefings.

k. 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).

2-6. Immediate Commanders/Supervisors. Immediate commanders/supervisors are responsible for the following:

- a. Designating sensitive positions.
- b. Assisting employees in obtaining help when they are experiencing personal problems which may affect their eligibility to perform sensitive functions.
- c. Reporting any information to the security manager that may affect an employee's ability to perform sensitive functions.
- d. Suspending access to classified information or temporarily removing an individual from sensitive duties.
- e. 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.
- f. Giving recommendations on incidents submitted through JPAS.
- g. Ensuring all supervised personnel receive security education training and briefings, as required, for the proper performance of their assigned duties.
- h. Protecting personal information in investigative and other reports about the person.

2-7. Individuals. Individuals are responsible for the following:

- a. Familiarizing themselves with pertinent security requirements pertaining to their assigned duties.
- b. Recognizing and avoiding personal behavior that could result in their ineligibility for a position of trust.
- c. Promptly reporting information of a security significance, as identified in AR 380-67, paragraph 9-103

2-8. Co-Workers. 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.

2-9. Inspections.

- a. The Security Division will conduct announced personnel security inspections yearly. Spot checks and unannounced inspections will be conducted by a Security Division representative, as necessary. A copy of the inspection results will be maintained on file within the activity until the next comparable inspection. The Inspection Checklist can be found at appendix A of this pamphlet.

b. All personnel performing personnel security functions are expected to be thoroughly knowledgeable in their area of responsibility. Additionally, a representative sampling of individuals occupying sensitive positions will be queried concerning their assigned duties and their awareness of the standards of conduct required of individuals 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 A of this pamphlet. 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 year. A copy of the inspection results will be maintained on file within the activity and subject to review by a representative of the Security Division, DPTMS.

2-10. Advice and Assistance Visits. The Security Division, DPTMS, will conduct, advise, and assistance visits upon request or as needed. Courtesy inspections will be conducted upon request or as deemed appropriate by Security Division but will not be conducted once the activity has been officially notified of a forthcoming inspection.

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 1-6. This official shall be responsible for the administration of an effective Personnel Security Program in that activity and possess, as a minimum, a validated SECRET security clearance and be a commissioned officer, warrant officer, noncommissioned officer (NCO) (SFC or above), or DA civilian (GS-07 or above, in NSPS equivalent to a GS-07 or above). A copy of the appointment will be provided to Security Division, DPTMS.

b. Requests to waive the minimum rank/grade requirements for designation of security manager will be forwarded to the Chief, Security Division, DPTMS. A sample memorandum is found in the Fort Knox Reg 380-5 (appendix O).

3-2. Supplemental Personnel Security Standing Operating Procedures (SOP). Written internal personnel security procedures must be established within each activity. These procedures should encompass instructions for each activities 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 SOP of all deployable units. This is normally covered under the Operation Security Program (OPSEC) and encompasses all the security procedures used in a field element, at appendix B of this pamphlet.

3-3. Routing of Personnel Security Actions. Personnel security actions on military and civilian personnel will be processed through the Personnel Security Branch, Security Division, DPTMS, or documentation will be forwarded to Security Division indicating security action was processed.

3-4. Limit Investigations and Security Clearances. Requests for personnel security investigations/security clearances will be limited to those essential to current operations or required for a specific military occupational specialty (MOS)/occupational skill, and clearly authorized by AR 380-67. A list of sensitive MOS/occupational skills is at appendix C of this pamphlet.

3-5. Cancellations. Personnel security actions will be canceled when no longer required. Request for cancellations will include full identifying data, action requested, and reason for the cancellation (i.e., deletion from Centralized Assignment Procedures (CAP) III assignment, transfer, or discharge). Cancellation can also be accomplished by calling the security office and supplying them the name and reason for cancellation. The security office will then cancel the open investigation. If the individual is being separated from active duty, indicate the basis for the separation and whether the individual will have a reserve obligation or enter into the National Guard.

3-6. Suspense Dates.

a. Suspense dates will be monitored and forwarded in order to reach the Security Division on the due date. If a suspense date cannot be met, arrangements for an extension should be made with a representative of the Personnel Security Branch before the due date.

b. Personnel security actions required in accordance with (IAW) CAP III must be processed as expeditiously as possible. DA has imposed a 21-day suspense, and this cannot be extended. Reason for noncompliance with CAP III actions must be fully documented

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. FK 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. The LRC can be no older than 60 days upon receipt of the action at Security Division, DPTMS. Any problems encountered with receiving results of the LRC in a timely manner that cannot be resolved at the requester's level shall be referred to the Security Division. The LRC consists of the following:

(1) Military personnel file (MPF) or official personnel file (OPF) will be screened by the S2/security manager or an authorized representative. The OPF should be reviewed for an existing record of an investigation that was previously completed if one is not shown in JPAS. The OPF and MPF should be reviewed 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 in JPAS. Refer to paragraph 1-4, this pamphlet, for a current definition of "Federal Service." Federal Service dates must be verified through enlistment/employment records maintained in the MPF or OPF. Dates reflected for basic pay entry date, basic active service date, or civil service computation date cannot be used, because those are adjusted dates.

(2) Medical records will be screened by a 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 as a U.S. military medical officer, a U.S. civilian physician under DOD contract or employed by the U.S. Government, or other qualified non-physician medical personnel (officer or enlisted) specifically designated by the supported U.S. military medical treatment facility. The Health Insurance Portability and Accountability Act (HIPAA) will be adhered to, and derogatory information will only be identified by a checkmark in the "Adverse or derogatory information summarized below" block on the LRC. It will then be the responsibility of the commander, director, or division chief to obtain additional information by requesting a Release of Information through the patient administration coordinator at the medical facility. If the civilian employee is also a retiree or dependent, indicate this information on the FK Form 1947 in the block GRADE/RANK.

(3) Military police and local intelligence files will be screened by authorized representatives of Directorate of Emergency Services/Law Enforcement Command/Provost Marshal (DES/LEC/PM) and Security Division, DPTMS, respectively, if the person has been in the geographic area for more than 30 days. These checks are not required for an individual on post less 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 are no longer available.

b. If an LRC cannot be/is not accomplished (i.e., 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 FK Form 1947 is provided at appendix D of this pamphlet. Locations of pertinent records are provided at paragraphs 3-7a(1), (2), and (3) of this pamphlet. The form must be typed or legibly printed and signed by the security manager or authorized representative. Include your office symbol 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. 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 the Security Division, DPTMS, (INTEL RCDS) or DES (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.

d. The FK Form 1947 can be downloaded from the Fort Knox Homepage (www.knox.army.mil/PUBS.htm) under Fort Knox Forms.

3-8. Central Clearance Facility (CCF) Telephone Terminal. Representatives of the Personnel Security Branch are the only individuals authorized to contact CCF.

3-9. Citizenship.

a. Proof of U.S. citizenship must be obtained before initial nomination for a security clearance. AR 380-67, paragraph B-4d, 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 E of 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 and provided an acceptable document as outlined in AR 380-67 and was used by the recruiter. There is no requirement to re-verify the citizenship of personnel previously verified (individual with a previous clearance listed in JPAS) unless there is reason to doubt the authenticity of the document or information.

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 or equivalent to a GS-07 and above (in NSPS equivalent to GS-07 or above). This function would normally be performed by the security manager.

c. Records must be maintained which specify who and what documentation were used to verify an individual's U.S. citizenship. The reverse side of FK 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.

d. Before acceptance and subsequent granting of access, be 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.

e. 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, the Republic of the Marshall Islands, and the Republic of Palau are no longer recognized as having U.S. citizen/national status. All were declared to be citizens of their countries. Reference AR 601-201, 7 June 2007.

f. 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.

g. Any legal questions concerning naturalization and citizenship requirements should be addressed to Legal Assistance, Staff Judge Advocate, 624-2771.

3-10. 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.

3-11. 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 F, although specifically oriented for the SCI pre-nomination interview; this guidance can be used for all PSI processing reviews. A sample subject interview worksheet using this guidance is provided at appendix F of this pamphlet.

3-12. Social Security Numbers Transmitted Over the Intranet. When transmitting Personnel Identifying Information and sensitive information over the Intranet, you must use your Common Access Card (CAC) and encrypt your message.

Chapter 4 Designation of Sensitive Positions

Section I General

4-1. General.

a. Certain positions involve duties of such a sensitive nature that 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 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, 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 Non-Sensitive (NS), Noncritical-Sensitive (NCS), Critical-Sensitive (CS) or Special Sensitive (SS). The criteria to be applied in designating sensitive positions are identified in AR 380-67, paragraph 3-101, and appendix G of this pamphlet. Specific criteria for assigning information technology (IT) I, II, or III positions and how to apply the criteria is provided at paragraph G-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. The NS positions need no formal approval. The cdr/director of your activity is the approving authority for all positions designated as sensitive. Once approved, the positions cannot be downgraded or reclassified without approval by the cdr/director of your activity. 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. Detailed instructions are contained at paragraph G-3 of this pamphlet and a sample SF 52-B provided at page G-6.

b. Once approved, assign a control number to the SF 52-B. 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. Furnish the Security Division, DPTMS, a copy of the approved SF 52-B.

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 item that will be covered in the yearly inspection.

4-5. Position Sensitivity Roster. A roster of sensitive positions will be prepared and maintained by the security manager. Prepare the roster bi-annually (January and July). Furnish a copy of the roster to the Personnel Security Branch. 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 a copy of the corrected roster. 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 page G-8 of this pamphlet.

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 stage of initiation and/or completion of required investigation before subject's appointment, along with exception to policy, is outlined in AR 380-67, chapter 3, section II. 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 to the required sensitivity, it is the responsibility of the hiring official, in coordination with the Human Resource clerk of the activity, as well as the activity security manager, to ensure the individual selected for a sensitive or non-sensitive position meets the prerequisite investigation/clearance requirement to occupy that position.

a. Exception to Policy. An exception to policy is required prior to the new hire starting the new position for NCS, CS, or SS if the following apply:

(1) An exception to policy is required for an NCS if the individual does not have a pre-requisite investigation or has more than a 2-year break in federal service. The investigation that meets the pre-requisite is the National Agency Check with Written Inquiries (NACI), Single Scope Background Investigation (SSBI), or SSBI-Periodic Reinvestigation (SSBI/PR).

(2) For an NCS, an exception to policy or investigation is not required if the individual has less than a 2-year break in service and has either an SSBI or SSBI-PR).

(3) An exception to policy is required for CS positions if the individual does not have a pre-requisite investigation or has more than a 2-year break in federal service. The investigation that meets the pre-requisite is the SSBI or SSBI/PR.

(4) Individual will be notified by CPAC 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 the employee's OPF pending granting of a final security clearance/completion of favorable investigation.

b. Types of Exception to Policy. The type of request for the exception to policy can be requested based on the position and requirements for the position. Samples of the exception to policy can be found at appendix H of this pamphlet.

(1) An exception to policy requiring an interim is requested if the duty position requires access to classified (page H-1 of this pamphlet).

(2) An exception to policy is requested not requiring an interim if the individual is in a position that has sufficient work to keep him/her gainfully employed until the clearance is granted (page H-2 of this pamphlet).

(3) An exception to policy is requested based on the fact the civilian employee is prior military and has a current NACLIC or SECRET/PR, less than a 2-year break in service, and the ANACI has been submitted. An Interim Clearance is not required (page H-3 of this pamphlet).

(4) An exception to policy is requested for an NCS position for a subject whose duties require an ANACI investigation but not a clearance.

c. If an exception to policy is granted, Security Division, DPTMS, will notify the activity security manager/S2 and CPAC.

Section III Military Positions

4-8. Personnel Security Requirements. All military positions will be reviewed by commanders and supervisors for personnel security requirements. The same criteria identified for civilian positions can be used.

(This page intentionally left blank)

Chapter 5

Requesting Personnel Security Investigations

Section I

General

5-1. Security Clearance Categories. Investigative requirements for the three security clearance categories (TOP SECRET, SECRET, and CONFIDENTIAL) are outlined in AR 380-67, paragraph 3-401. Before initiating a request for investigation, ensure the subject of the investigation will have sufficient time remaining in the service or in the position after completion of the investigation warrants conducting it.

5-2. Execution of the Investigation. Security managers will ensure request forms are properly executed utilizing JPAS and e-QIP.

a. Security managers will conduct local files checks on all investigations requiring a security clearance prior to submission of the investigation.

b. Security managers will initiate the investigation utilizing JPAS. Follow the JPAS Instructions in appendix I of this pamphlet. See work-around instructions in appendix K of this pamphlet for new civilian hires, civilian applicants, and ROTC cadets.

c. Subject will be given a copy of appendix J (Subject's e-QIP Quick Reference) of this pamphlet. Subject will be instructed that the e-QIP must be started within 30 days of initiation and must be completed within 90 days.

d. Security managers will review the completed e-QIP SF 86 to ensure all items are properly completed and explained in sufficient detail where the subject understands information requested and its importance. After subject has followed the Subject's e-QIP Quick Reference, he/she will submit the investigation to the security manager by selecting the "Release Request/Transmit" button in e-QIP (see appendix K of this pamphlet).

e. The security manager will follow JPAS instructions for transmitting the investigation to the Office of Personnel Management (OPM). Forward a copy of the Add/Modify notification indicating the PSQ has been sent to the Security Division. If fingerprints are required, forward them with the Add/Modify notification to the Security Division. When the Security Division starts utilizing the digital fingerprint scanner, forward the Add/Modify notification indicating the PSQ has been forwarded.

Section II

Types of Investigation and Forms Required

5-3. Entrance National Agency Check (ENTNAC)/National Agency Check (NAC). An ENTNAC was conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. Since 1 Jan 99, the investigation has been changed to a NAC. The ENTNAC or NAC for inductees is accomplished by the U.S. Army Recruiting Command. It is

the responsibility of the G1/Adjutant General to ensure that no Soldier departs from initial entry training or one station unit (OSUT) site until results of the ENTNAC/NAC have been received and are documented. An NAC/ENTNAC **cannot** be used as a basis for granting a SECRET or CONFIDENTIAL security clearance.

5-4. National Agency Check (NAC). NACs are conducted on contractors that require an investigation for public trust positions and access to Government computers along with Non-Appropriated Fund (NAF) employees. For contractors, the contract security manager or the activity security manager will notify this office requesting initiation of a NAC (supplying the name and social security number). The Security Division will initiate an investigation and instruct the security manager to supply the subject with appendix J of this pamphlet (Subject's e-QIP Quick Reference). After subject completes the investigation, it will be reviewed by the security manager prior to notifying the Security Division. The Security Division will contact the subject for fingerprinting (when the digital scan is in operation) (see appendix L of this pamphlet for a sample fingerprint card) then forward the NAC to OPM. The NAF, Civilian Personnel Office, initiates the investigation for NAF employees. A NAC consists of the following forms:

- a. The e-QIP SF 85P.
- b. One FD 258 fingerprint chart.

5-5. National Agency Check, Local Agency Checks, and Credit Check (NACLCL). An NACLCL is required for military personnel to obtain a SECRET or CONFIDENTIAL Security Clearance. The NACLCL has been in effect since 1 Jan 99. Some initial entry trainees are also required to have NACLCLs conducted on them upon entrance into the service. The NACLCL conducted by OPM consists of a financial review by verification of subject's financial status, including credit bureau checks, covering all locations where the subject has resided, been employed, and attended school for 6 months or more during the past 7 years. The OPM will conduct a Local Agency Check; as a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last 5 years, and, if applicable, the appropriate agency for any identified arrests. An NACLCL is initiated by the security manager/S2 and consist of the following:

- a. The e-QIP SF 86.
- b. One FD 258 fingerprint chart.

5-6. SECRET Periodic Reinvestigation (SECRET/PR). The SECRET/PR program is an ongoing program. At the 10-year mark of the investigation, the clearance is downgraded to CONFIDENTIAL, and at the 15-year mark, the clearance is terminated. When an individual's investigation is over 10 years old and the individual occupies an NCSS position, deployment requirement, or their MOS requires a SECRET clearance at the anniversary date, the SECRET/PR must be initiated. If the individual requires a CONFIDENTIAL clearance, the SECRET/PR must be submitted at the 15-year anniversary date. A SECRET/PR is initiated by the security manager/S2 and consist of the following forms:

- a. The e-QIP SF 86.
- b. One FD 258 fingerprint chart if the previous investigation was an ENTNAC.
- c. If an FD 258 is not required, annotate on the SF 86, Authorization for Release of Information form under "Other Names Used" the following statement: "This is a Secret/PR. No fingerprints are required."

5-7. National Agency Check with Written Inquiries (NACI). An NACI is conducted on each Federal Civil Service employee at the time of appointment. This is accomplished by the Civilian Personnel Office. An NACI will not be requested by CPAC if the employee is placed into an NCS position (see paragraph 5-9 below) or CS position (see paragraph 5-10 below) or was the subject of a previous SSBI and there is not a break in Federal service greater than 24 months. A security clearance will **not** be granted based on an NACI. An NACI consists of the following forms:

- a. SF 85 (Questionnaire for Nonsensitive Positions).
- b. One SF 87 (fingerprint chart).
- c. Resume.
- d. OF 306 (Declaration for Federal Employment).

5-8. Access National Agency with Written Inquiries (ANACI). An ANACI must be submitted on all newly-hired civil service employees occupying an NCS position or civil service employees who do not have a security clearance and changed positions where they require a SECRET or CONFIDENTIAL clearance. An ANACI consists of the following forms:

- a. The e-QIP SF 86.
- b. One SF 87 (fingerprint chart).
- c. Resume.
- d. OF 306 (Declaration for Federal Employment).

5-9. Single Scope Background Investigation (SSBI). An SSBI is the investigation used for individuals occupying CS positions. This investigation is required to obtain a TOP SECRET clearance and access to SCI. The SSBI is initiated by the security manager/S2. An SSBI is not submitted on individual's due to rank or just to obtain a TOP SECRET clearance. It is submitted only when the duty position requires a TOP SECRET clearance or because of MOS or deployment requirements. The SSBI consist of the following forms:

- a. The e-QIP SF 86.

- b. Two FD 258s (fingerprint charts).

5-10. Periodic Reinvestigations (PRs). The PR is an SSBI periodic reinvestigation. The PR program is an ongoing program. At the 5-year mark of the investigation, the clearance is downgraded to SECRET, and at the 10-year mark the clearance is downgraded to CONFIDENTIAL, and at the 15-year mark the clearance is terminated. When an individual's investigation is over 5 years old and the individual occupies a CS position or their MOS requires a TOP SECRET clearance at the anniversary date, the PR must be initiated. PRs are not submitted on individuals due to rank or just to retain the TOP SECRET clearance. They are submitted on duty position, MOS, or deployment requirements.

- a. The e-QIP SF 86.
- b. Fingerprints are **not** required.
- c. Do Not Submit SECRET/PR's or PRs. If an individual is within 12 months of retirement, the SECRET/PR or PR will not be submitted. The individual will keep his/her current security clearance.

5-11. Failure or Refusal to Complete a SECRET/PR or PR.

a. An individual who refuses or neglects to submit the completed investigative 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 revocation of the security clearance. The revocation of a security clearance could result in 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 an Incident Report reported in JPAS. Indicate in the Incident Report reason(s) for non-submission.

5-12. Fingerprinting. Fingerprints are currently conducted by PMO. The designated date and time is Mondays 0900-1100. Appointments for fingerprinting can be made by calling 624-4040. Security Division will be obtaining and utilizing a fingerprint scanner in the near future and will contact you when it becomes available. The OPM will not open an investigation until they receive the fingerprint chart shown in appendix L of this pamphlet. Forward the fingerprint charts to this office along with the Add/Modify notification from JPAS (see appendix K of this pamphlet) the day the electronic investigation is forwarded in JPAS.

5-13. Civilian Investigations versus Military Investigations. There seems to be some confusion about a military investigation and clearance remaining valid when the individual becomes a civil service employee. Every civil service employee must have, as a minimum, a NACI; the NACLIC, ENTNAC, or NAC will **not** suffice. If the prior investigation was an SSBI

or PR, less than a 2-year break in federal service, the investigation is valid for a civil service employee, and a NACI is not required.

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

(This page intentionally left blank)

Chapter 6

Requesting Security Clearance and Granting Access

Section I

Requesting Security Clearance

6-1. Granting Authority. The Commander, Central Clearance Facility (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, Security Division, DPTMS. Policies governing security clearances are outlined in AR 380-67, section IV.

6-2. Limitations. Requests for security clearances will be limited only to U.S. citizens who require access to classified information for mission accomplishment and the requirement for civilians who have been identified on the Civilian Sensitivity Roster. 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). 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.

6-4. Interim Security Clearances. 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. When a person requires an interim security clearance, security managers will submit a request for security clearance utilizing DA Form 5247-R (Request for Security Determination). Instructions for completing the form are contained in appendix M of this pamphlet.

a. Requests for interim security clearances should be kept to a minimum and must contain full justification.

b. Per JPAS procedures, dated 14 Feb 05, interim access may be granted after the Personnel Security Investigation is submitted to the OPM. The date the clearance is effective as shown in the Person Category Screen in JPAS. Interim clearances remain valid until access is no longer required or clearance is granted by the CCF.

c. Interim clearances are not required for newly hired civilians who have a current NACLIC or SECRET/PR, SSBI, or PR with less than a 2-year break in service and the appropriate investigation has been submitted.

d. Individuals with outdated investigations who previously had a SECRET security clearance (reflected in the JPAS eligibility screen) and had less than a 24-month break in federal service after submission of their NACLIC/PR or SSBI/PR with no significant derogatory information, will retain their clearance at either the SECRET or TOP SECRET level, regardless of the age of the previous investigation. An interim clearance will not be required for these individuals. If derogatory information is contained in the reinvestigation, it must be reviewed by the Security Division, DPTMS, before access can be granted.

6-5. Personnel Security Actions for Reassignment.

a. Personnel Reassignment Section, AG, will provide Security Division, DPTMS, a hard copy of each reassignment instruction requiring a personnel security action.

b. Security Division will notify the unit S2/security manager of the required personnel security action and date the action must be completed.

c. The unit S2/security manager 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/security manager, would disqualify the individual for a security clearance/special access or reassignment, will be reported immediately to the 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.

d. Upon completion of the personnel security action, Security Division will notify the Personnel Reassignment Section that the required investigation and interim clearance, if requested in the assignment, has been processed.

e. The Security Division will notify Personnel Reassignment Section upon completion of all security clearances required before orders can be issued and the individual can deploy.

6-6. Promotions Based on Rank/MOS. The following security clearance requirements are a prerequisite for promotion based on AR 600-8-19, paragraph 1-15:

a. Promotion to MSG and SGM requires an INTERIM SECRET clearance or higher.

b. Promotion to SPC through SFC clearance requirement is dictated by the MOS .

6-7. Officers Security Requirement. All officers will maintain a current SECRET clearance at Fort Knox, as a minimum. TOP SECRET clearances are based on specific duty requirements -- not based on rank.

Section II
Granting Access

6-8. Accepting a Validated Clearance.

a. Access to classified information can be granted to individuals whose official duties require such access and have the appropriate personnel security clearance which has been accepted by the S2/security manager. Security managers can accept a clearance granted in the JPAS based on the following:

(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. 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.

c. An initial security briefing is required before the individual can have access to classified information. The initial security briefing can be found at appendix U of this pamphlet.

6-9. Access Authorization/Documentation of Security Clearance Using FK Form 1378.

a. Access will be indicated in the JPAS in the Person Summary Screen under Accesses (Indoctrinate Non-SCI). Access will be granted after verifying the non-disclosure statement is annotated in JPAS. Once an individual departs the unit/organization, the access is removed under De-brief Non-SCI. They do not execute a de-briefing statement.

b. A validated clearance in JPAS is considered by this command as officially accepted upon signing and dating of FK Form 1378, Record of Personnel Security Clearance/Action. The FK Form 1378 should be completed when an individual occupies a sensitive position or requires access to classified information within an activity. Detailed instructions for completion of FK Form 1378 are contained in appendix N of this pamphlet.

c. FK Form 1378 will be destroyed 30 days after permanent change of station (PCS) or expiration of term of service (ETS)/retirement of the individual. For on-post transfers, forward the FK Form 1378 to the gaining activity's S2/security manager.

6-10. Security Access Roster (SAR). The SAR is an inclusive access roster which includes military and civilian employees who have a validated (accepted) security clearance within your activity along with those occupying an MOS that requires a security clearance. An updated SAR must be forwarded to the Security Division, DPTMS, every January and July. It does not replace the Civilian Sensitivity Roster. A sample format of the roster is provided at appendix O of this pamphlet.

6-11. Verification of Security Clearance/Access Authorization for TDY Personnel.

a. Upon issuance of orders for TDY, the clearance date should be verified by the security manager prior to publication of the order.

b. Access to SCI at the TDY site must be verified by the Special Security Office (SSO), Security Division, DPTMS. Telephone numbers for the SSO are 624-1425/5529 (DSN 464-1425/5529).

6-12. Visit Requests

a. Visit Authorization Letters (VALs) are no longer required for visits involving civilian, military, and contractor personnel whose access level and security management office (SMO)

affiliation are accurately reflected in JPAS. Visit requests submitted through JPAS will not be accepted if they do not reflect accurate access, "NDA Date," and appropriate SMO identification. JPAS should be used for passing of visit access authorizations in order to lessen the administrative burden and capitalize on the expediency and efficiencies gained by utilizing electronic means. Continued use of written visit request letters for visit access control purposes is authorized only when electronic means is not available or if an individual is not in JPAS.

b. The command sponsoring the visitor (command/activity who has either an owning or servicing relationship with the individual who intends to visit another activity) is responsible for ensuring and validating the accuracy of the access and affiliation data in JPAS before initiating the visit request. See instructions for entering visit requests in appendix I of this pamphlet (JPAS instructions).

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. The Director, Defense Intelligence Agency (DIA), is responsible for direction and control of SCI Security Programs established by DOD components.

7-2. SCI Access. Request access justifications should be forwarded to the Chief, Security Division, DPTMS, in the format shown at appendix P of this pamphlet. The justifications must clearly establish a mission-related need for access to SCI material. No person will be deemed to have a need-to-know solely by virtue of rank, title, or position.

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.

b. 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 proposed date of marriage, along with any affiliation to any foreign national, to include relationship and nationality, must be included in the SSBI packet.

c. The investigative requirement for access to SCI is an SSBI or conducted where there has been no break in Federal service greater than 24 months since the SSBI was conducted.

d. If it is determined the nominee does not possess a current SSBI, a SSBI packet (or SSBI PR, as appropriate) will be submitted through JPAS.

7-4. Nomination Procedures. Individuals requiring SCI access should be nominated as soon as they are identified. Nominations will be submitted through the senior intelligence officer to SSO.

a. Choose individuals who can fill positions for a considerable period of time. Nominations should not be submitted on personnel who would have less than 1 year tenure after SCI indoctrination.

b. In most cases, access is given for an extended period. Exceptions are nominations for one-time access to attend a conference or briefing or other situations which temporary (no more than 180 days) SCI access appears warranted. 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 P of this pamphlet.

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 3-501d. 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 an individual 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 P of this pamphlet.

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

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

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

(4) Favorable review of local files.

(5) Initiation of the SSBI (received by OPM).

(6) 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 for the position the individual will occupy and may only request the type of accesses required.

7-6. Indoctrination.

a. The nominated individual will be indoctrinated by SSO upon receipt of authorization from the Cdr, CCF.

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, Bldg. No. 1109-A, at the time scheduled for indoctrination.

c. At the time of indoctrination, the SSO will levy certain special requirements regarding travel restrictions, assignment restrictions, and 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, including 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 changeover to have the outgoing and incoming individuals indoctrinated for a period not to exceed 90 days.
- e. Individuals granted access to SCI will receive a security awareness briefing annually.

7-7. Debriefing. Appointment for debriefing must be coordinated with SSO when a person 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 and send the Incident Report (IR), submitted through JPAS, to Security Division, DPTMS. 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, Security Division, DPTMS.

Section II

Nuclear Weapons Personnel Reliability Program (PRP)

7-9. Governing Regulation. AR 50-5, Nuclear Surety, sets forth the policies, procedures, and responsibilities for implementing the Army Nuclear Surety Program.

7-10. Investigative Requirements. Investigative and certification requirements for personnel performing duties associated with nuclear weapons are addressed in AR 50-5, Chapter 2, Section IV, paragraph 2-14.

7-11. Supplemental Guidance.

a. Service academy cadets are considered the same as active duty military 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. Pre-requisite security clearance/investigation for attendance at Phase I, EOD School, is SECRET/SSBI. Students must arrive with a minimum clearance of an INTERIM SECRET with an SSBI initiated. If an individual 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 SECRET clearance along with e-QIP SF 86 form for review.

d. Request for dossiers should be submitted using DA Form 5247-R to Security Division, DPTMS. The request must include the subject's name (LAST, First MI), date of birth, state or country of birth, social security number (SSN), and justification.

Section III Chemical Surety

7-12. Governing Regulations. AR 50-6, Chemical Surety, prescribes policies, procedures, and responsibilities for the Chemical Surety Program.

7-13. Investigative Requirements. Personnel security investigations and clearance requirements are outlined in AR 50-6, Chapter 2, Section IV, paragraph 2-13.

Section IV Information Systems Security

7-14. Governing Regulations. Minimum investigative requirements for personnel performing IT functions as outlined in AR 380-67, paragraph 3-614, and AR 25-2, Section V, paragraph 4-14, are listed below.

7-15. Investigative Requirements. Investigative requirements are as follows:

- a. IT-I: SSBI. Favorable completion of a NAC portion is current with 180 days.
- b. IT-II: NACLC or ANACI.
- c. IT-III: NAC or NACI.

7-16. Network Access and Security Clearance Suspension/Denial/Revocation. The network access is governed by AR 25-2, Information Assurance. The Fort Knox policy for Network Access can be found in detail under the Fort Knox Homepage (<http://147.238.100.101/>) under Fort Knox Policy Memorandums based on Chapter 4, Section V, Personnel Security paragraph (b4).

Section V

Access to North Atlantic Treaty Organization (NATO) Classified Information

7-17. Governing Regulations. 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.

7-18. Investigative Requirements

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. The investigative requirement falls under the 5-year reagency requirement. Before receiving the NATO briefing, the activity security manager/S2 will prepare a written request to Security Division, DPTMS. The request will give the name of the individual, SSN, degree of U.S. security clearance/date granted, degree of local access/date granted, type of investigation/date of investigation, and justification. Upon receipt of the request, Security Division, DPTMS, 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. The activity security manager must contact Security Division, DPTMS, to arrange for debriefings.

Section VI

Critical Nuclear Weapon Design Information (CNWDI).

7-19. Governing Regulation. Policy for access to and dissemination of CNWDI is outlined in AR 380-5, Access to and Dissemination of Restricted Data (Chapter 6). CNWDI is extremely sensitive, and access must be limited to the minimum number of individuals who need it to accomplish their assigned mission.

7-20. Briefing and Debriefing. Per AR 380-5, briefing and debriefing will be executed by the security manager. A sample briefing for CNWDI access can be found in the AR 380-5, Chapter 9-13. A Security Termination Statement and Debriefing Certificate, DA Form 2962, will be signed by the individual when access is no longer required to CNWDI. On the DA Form 2962, under Part III, check Other and explain this is a debriefing for CNWDI even though the individual is not separating or retiring from service.

Section VII
Special Access Program (SAP)

7-21. Governing Regulations. Policy for access to and dissemination of the SAPs and Sensitive Activities is AR 380-381. The Joint Air Force-Army-Navy (JAFAN) 6/4 is also a reference to the SAPs.

Chapter 8

Unfavorable Administrative Actions

Section I

Reporting of Unfavorable Information

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

8-2. Primary Responsibility. 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. Definition. 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 Q of this pamphlet. 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. Sources. 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 (SIRs);
- 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, Courts Martial, 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. Reporting Procedures. Derogatory information surfaced at the local level on assigned/attached military and DOD civilian personnel must be reported as it becomes known. Extreme caution should be exercised to ensure the information reported is complete and accurate. AR 380-67, appendix I, and DOD Adjudication Guidelines contain 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 the DOD Adjudication Guidelines, should be reviewed before submitting a final report to ensure all information required to make a final adjudication has been provided.

a. The vehicle used for reporting credible derogatory information is reported through JPAS (see appendix I of this pamphlet under Report Incident for instructions). When an initial IR is submitted, follow-ups or finals will be submitted 90 days after the initial report to the CCF, as well as the Security Division, DPTMS. A final report can be submitted instead of an initial if the incident has been closed and all action completed. One copy of the initial, follow-up, or final plus any enclosures that are faxed (DSN 622-2706 or 301-677-2706) to CCF are to be furnished to the Security Division, DPTMS. See examples of Reportable Information in appendix Q of this pamphlet.

b. The DA Form 5248-R (Report of Unfavorable Information For Security Determination) will be used only if a separation date is shown in JPAS and the incident cannot be put in JPAS (sample at appendix R of this pamphlet). Attach any enclosures to the 5248-R and forward to the Security Division, DPTMS.

c. Complete detailed information must be provided to enable the CCF adjudicators to make a final security determination. Always give the WHO, WHAT, WHEN, WHERE, and WHY when completing a final IR.

d. The commander can give his/her recommendation as to whether the individual should have his/her clearance revoked or keep the clearance. If the commander recommends suspending access as a result of the incident, call the Security Division for guidance. Once the access is suspended in JPAS, it can only be removed by CCF. **DO NOT SUSPEND THE CLEARANCE WITHOUT SECURITY DIVISION'S ACKNOWLEDGEMENT.**

8-6. Alcohol Incident. When reporting an alcohol incident, you must include on your IR the referral or attendance to Army Substance Abuse Program (ASAP) (indicate attendance and successful completion of the program, along with date). All alcohol- and driving-related incidents have a mandatory referral for an evaluation and education per AR 190-5 and AR 600-85, 2-1c.

8-7. Misuse of Government Travel Card. Misuse of the Government travel charge card must be reported via IR. If an individual is delinquent in paying his/her Government travel card account balance or there is misuse of the card, it must be reported to CCF.

8-8. Misuse of Government Computer. The Adjudication Guidelines contains the reporting of Misuse of Information Technology Systems (Guideline M). When an individual is identified

and "blackholed" by DOIM and their account is disabled, various steps will be taken before the individual can be given access to the computer. The command will conduct an investigation, and after the investigation is complete, the security manager will do one of the following:

- a. Complete an IR in JPAS if disciplinary action is taken.
- b. If no disciplinary action is taken, an IR is not required. Notify the Security Division, DPTMS, that no action is taken.

8-9. Unauthorized Absence or Suicide. 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, Chapter 10 "Unauthorized Disclosure and Other Security Incidents," paragraph 10-9, to detect if there are possible security implications. The results of the inquiry will be included in your report of unfavorable information.

8-10. Release of Information. 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.

8-11. Security Manager Responsibility. 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

8-12. Governing Regulation. Suspension of access to classified information is addressed in AR 380-67, paragraph 8-102.

8-13. Purpose of Suspension of Access. 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, or 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.

8-14. Formal/Informal Suspension. 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.

a. Informal suspension can be used as an interim measure while gathering information to determine whether formal suspension is warranted. Options pertaining to suspension and supplemental procedures are as follows (see appendix S of this pamphlet):

(1) If access is granted in the Person Summary Screen, it can be removed until a decision is made whether to grant access based on the information gathered.

(2) Access may be reinstated by suspending official.

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

b. Formal suspension should be taken when information exists which raises serious questions as to the individual's ability or intent to protect classified information. **DO NOT SUSPEND THE CLEARANCE WITHOUT SECURITY DIVISION'S ACKNOWLEDGEMENT.** In a formal suspension, access is suspended in JPAS under the Report Incident Screen and 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, DPTMS.

8-15. Guidance Upon Suspension of Access. Upon suspension of access, the S2/security manager must take the following actions:

a. Notify the individual concerned in writing that access to classified information has been suspended and the reasons for suspension. A sample format is provided at appendix S of this pamphlet.

b. Delete the individual's name from all access rosters (FK Form 1378 must be removed from the active file, lined through, and a notation made as to suspension of access).

Section III

Unfavorable Administrative Action Procedures

8-16. Governing Regulation. Unfavorable administrative action procedures are addressed in AR 380-67, section II.

8-17. Letters of Intent. 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, DPTMS, 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.

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; other lawyers (at the individual's expense); or from his/her unit commander/supervisor and activity S2/security manager, as well as Security Division.

c. If the individual intends to submit a rebuttal, he/she will be instructed to route the rebuttal through the appropriate chain of command to Security Division within 60 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 DOD 5200.2R, appendix G. A copy of the rebuttal guidelines is provided at appendix T of this pamphlet.

d. A copy of the LOI will be provided through security channels to the individual's unit commander or supervisor. 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 rebuttal and provide a recommendation as to whether the individual's security clearance should be denied, revoked, or restored. The commander/supervisor must provide rationale addressing 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 an 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 an 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 the individual'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 final decision will be forwarded through Security Division to the individual.

8-18. Appeals and Reconsiderations. Procedural guidance for requests for appeals and reconsiderations are addressed in AR 380-67, paragraphs 8-201d and 8-201.1, respectively. The rules concerning appeals and reconsiderations are as follows: (Appeals and reconsiderations are forwarded through the Security Division to the appropriate office.)

- a. Rule No. 1: Reconsideration requests go to CCF; appeals go to HQDA (DAMI-CIS).
- b. Rule No. 2: If subject of the action is providing additional information for consideration, it is a reconsideration request. If there is no additional information, it is an appeal.
- 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. The individual has the opportunity for a personal appearance before an administrative judge from the Defense Office of Hearing and Appeals (DOHA).

8-19. Security Manager's Responsibility. The S2/security manager has an obligation to assist the individual by ensuring the procedures are understood and followed and review the packet before submission to make sure it addresses the issues and complies with procedures.

8-20. Involuntary Separation. Involuntary separation of military members 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 Information (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. 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.

(This page intentionally left blank)

Chapter 9 Continuing Security Responsibilities

Section I Responsibilities

9-1. Evaluating Continued Security Eligibility. 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 regards to reporting matters of personnel security concern.

9-2. Standards of Conduct. 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 should take the following actions:

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 standards of military and civilian personnel who have access to classified information or perform sensitive duties. Additionally, a statement will be made on the person's annual performance report describing how the security responsibilities were discharged. Bullet examples are as follows:

- (1) Properly safeguards classified and sensitive information.
- (2) Handles personnel security records with the highest discretion.
- (3) Maintains high standards of personal conduct.

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, (appendix U of this pamphlet) and refresher briefings on an annual basis. The briefing will be conducted IAW 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/she should be informed of the degree of security clearance which was granted by Cdr, CCF, and the level of access required to

perform his/her assigned duties. A record of these briefings will be maintained by the S2/security manager. Item 13, FK Form 1378, should be used to record the initial briefing. Security Division has personnel training videos available for annual security training.

9-5. Nondisclosure Agreement (NDA). In accordance with AR 380-5, chapter 6-2, personnel granted a security clearance shall not be permitted to have access to classified information until they have signed SF 312, Classified Information Nondisclosure Agreement. If the person declines to execute the NDA, action must be taken to informally suspend the individual's access to classified information for a 5-day period, allowing the individual time to reconsider signing the NDA. At the end of the 5-day period, if the individual still declines to sign the NDA, the individual's access to classified information will be formally suspended and an IR will be submitted through JPAS. The IR must reflect the individual was given a 5-day period to reconsider signing the NDA. The date the NDA was executed should be reflected in item 13, FK Form 1378. The nondisclosure date will also be entered in JPAS in the Accesses block under Indoctrinate Non-Sci. Addresses to mail the original SF 312 for military personnel can be found in AR 380-5, paragraph 6-3(b). The original SF 312 for civilians will be forwarded to the Civilian Personnel Operations Center for placement in their OPF.

9-6. Foreign Travel.

a. All cleared personnel (military, DA civilian, contractor) holding a TOP SECRET security clearance and having access to SCI will report all personal, unofficial foreign travel to their security manager, as well as the SSO, 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 individuals who are cleared at the SECRET and CONFIDENTIAL level do not have to report personal foreign travel.

c. 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 prior to official OCONUS travel. Assistance in preparation of your foreign travel briefings can be obtained by contacting the Anti-terrorism Operations and Intelligence Cell at 502-624-6083/3101.

9-7. Termination Briefing.

a. Security managers are responsible for debriefing personnel per AR 380-67, paragraph 9-204. DA Form 2962 (Security Termination Statement and Debriefing Certificate) or SF 312 (Classified Information Nondisclosure Agreement) bottom back side will be used for this purpose. A sample copy of DA Form 2962 is provided at appendix V of this pamphlet.

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.

9-8. Change in Status of Individual.

a. If an individual is transferred to another organization on post, FK Forms 1378, if requested, should be transferred to the gaining command security manager. Security Division, DPTMS, should be notified of individual's location, when appropriate. When possible, IRs should be updated and/or finalized prior to individual's transfer. Closed case files may be destroyed.

b. Open/closed case files and FK Forms 1378 pertaining to personnel being reassigned off the installation should be destroyed.

c. Security Division, DPTMS, should be notified in writing or telephonically of all pending requests for security determinations/investigations that can be canceled due to the change in mission and/or reassignment.

d. 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).

(This page intentionally left blank)

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. Safeguarding the Information. 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. Listed below are the primary rules to follow:

- a. Restrict access to information contained in security files to those personnel in your activity that have an absolute need for access in connection with authorized personnel security actions.
- b. Maintain files in the security office using a proper security container or locking file cabinet.
- c. Destroy files upon separation or transfer of the individual.
- d. Do not allow the individual or anyone representing him/her access to the security files.
- e. If you are going to use information from the dossiers for an unfavorable personnel action, you may extract information from them, but you may NOT use copies of actual material from the dossiers without the permission of the files holding agency. 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, DPTMS, when you are contemplating using dossier information in an unfavorable personnel proceeding.

10-3. Requesting/Reviewing Investigative Dossiers.

a. The only activities at Fort Knox authorized to request and store personnel security investigative dossiers are the Security Division, DPTMS, and Trainee/Student Records at AG. Trainee/Student Records 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, DPTMS, IAW 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, DPTMS, via a 5247-R. The request must include subject's name, date of birth, state or country of birth, SSN, and justification.

c. A list of personnel authorized to review investigative reports on file within Security Division, DPTMS, will be submitted by the commander/director if other than the designated security

Fort Knox Pam 380-67 (24 Jul 08)

manager will be conducting the review. Appointment for review of files can be scheduled by contacting the Personnel Security Branch, 624-6741/2814.

10-4. Requesting Information Under Freedom of Information. If an individual requests to see or have access to information in his/her investigative files, he/she can request the investigative file through the OPM or Office of Freedom of Information:

a. THE COMMANDER, U.S. ARMY INTELLIGENCE AND SECURITY COMMAND IS AUTHORIZED TO ACT ON REQUESTS FOR INTELLIGENCE INVESTIGATION AND SECURITY RECORDS. A written request can be submitted to the following address:

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
(IAMG-CIC-FOI/PO)
4552 PIKE ROAD
FORT MEADE, MD 20755-5995

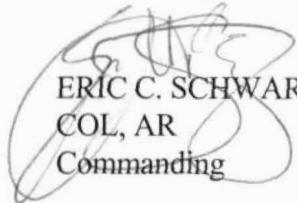
Include the individual's full name, SSN, date of birth, place of birth, and current home address. Requests can be sent to FAX number (301) 677-2956

b. The OPM has files that contain information gathered through an investigation submitted for either a clearance or an investigation for a position not requiring a clearance. They can submit a written request to FOIA/Privacy Act Group (OPM-FISD), PO Box 618, Boyers, PA 16018-0618. The request requires the individual's hand written signature, full name, SSN, date of birth, place of birth, and current home address. If the individual wants to fax the hand-signed request to OPM, it can be faxed to FOIA/Privacy Act Group (OPM-FISD), Boyers, PA at (724) 794-4590. Normal processing time is 20 days. If letter of intent/statement of reasons intention documentation is included with the request, the normal processing time is 5 days.

c. Requesters who seek access to Defense Security Records about themselves which are not background investigation affiliated (e.g., employment records) should cite the Privacy and FOIA and address inquiries to DSS, Office of FOIA and Privacy (Leslie Blake), 1340 Braddock Place, Alexandria, VA 22314-1651. Written inquiries can also be e-mailed to DSS at or FAXed to (703) 325-5991.

d. Additional information can be found under the JPAS homepage at www.dss.mil under DSS FOIA and Privacy Act.

10-5. Disposition of Other Personnel Security Actions. Personnel security actions shall be destroyed 60 days after the individual has departed this installation. Actions pertaining to on-post transfers shall be forwarded to the gaining command security manager/S2.


ERIC C. SCHWARTZ
COL, AR
Commanding



KENT R. SHAW
Director, Human Resources

DISTRIBUTION:
A

(This page intentionally left blank)

**Appendix A
Inspection Checklist**

INSPECTION CHECKLIST			
For use of this form, see Fort Knox Pam 25-31			
FUNCTIONAL AREA		SUBJECT AREA	
SECURITY		PERSONNEL SECURITY	
PROPOSER/PHONE NO.			DATE OF REVISION (MM-DD-YYYY)
Personnel Security Branch, Security Division, DPTMS			
UNIT INSPECTED		DATE (MM-DD-YYYY)	INSPECTOR'S NAME/PHONE NO.
YES	NO	N/A	INSPECTION ITEM
			<p>REFERENCES:</p> <ul style="list-style-type: none"> a. AR 380-67, The Department of the Army Personnel Security Program, 9 September 1988. b. Ft Knox Pamphlet 380-67, Personnel Security Program, 24 Jul 08. c. Current Personnel Security Updates. <p>PROGRAM MANAGEMENT:</p> <ul style="list-style-type: none"> 1. Has an official been appointed to serve as S2/Security Manager/Alternate (Ft Knox Pamphlet 380-67, para 3-1)? 2. Have comprehensive supplemental personnel security procedures been developed which comply with Ft Knox Pamphlet 380-67, para 3-2 and appendix B? 3. Has a program been established for self-inspection and periodic oversight inspections of subordinate elements (AR 380-67, para 11-101h(7), and Ft Knox Pamphlet 380-67, para 2-9d)? <ul style="list-style-type: none"> a. Are the subordinate inspections conducted, at a minimum, once every year? b. Are inspection results placed in writing and available for review? 4. Are supplemental questionnaires/checklists being used as an evaluation procedure in support of the Personnel Security Program (Ft Knox Pamphlet 380-67, para 3-11 and appendix I)? 5. Are S2/Security Managers thoroughly familiar with pertinent regulations and the responsibilities of their position (Ft Knox Pamphlet 380-67, para 2-5)? <p>DESIGNATION OF SENSITIVE POSITIONS:</p> <ul style="list-style-type: none"> 1. Have all civilian positions within the activity been categorized as nonsensitive, noncritical-sensitive, or critical-sensitive (AR 380-67, para 3-101, and Ft Knox Pamphlet 380-67, para 4-2)? <ul style="list-style-type: none"> a. Have the sensitive positions been approved by the commander/director of your activity (Ft Knox Pamphlet 380-67, para 4-3)? b. Are approved copies of the SF 52s on file within your activity (Ft Knox Pamphlet 380-67, para 4-4b)? c. Are all changes affecting a sensitive position reported to the Personnel Security Branch (PSB), Security Division, DPTMS, as they occur (Ft Knox Pamphlet 380-67, para 4-4c)? d. Is an updated Civilian Sensitivity Roster furnished to PSB every January and July (Ft Knox Pamphlet 380-67, para 4-5)? e. Are personnel occupying sensitive positions properly cleared or an exception to policy granted before hire (AR 380-67, paragraph 3-204, and Ft Knox Pamphlet 380-67, paragraph 4-7).

INSPECTION CHECKLIST (continued)			
FUNCTIONAL AREA			SUBJECT AREA
SECURITY			PERSONNEL SECURITY
YES	NO	N/A	INSPECTION ITEM
			<p>2. Is an updated Security Access Roster (SAR) furnished to PSB every January and July (Ft Knox Pamphlet 380-67, para 6-9)?</p> <p>INITIATION OF PERSONNEL SECURITY ACTIONS:</p> <p>1. Are the number of individuals cleared for access to classified information kept to a minimum consistent with the requirements of operations or MOS/occupational skills (AR 380-67, para 2-501, and Ft Knox Pamphlet 380-67, para 5-15)?</p> <p>2. Are requests for clearances/investigations canceled when no longer needed (AR 380-67, appendix C-1e, and Ft Knox Pamphlet 380-67, para 3-5)?</p> <p>3. Are requests for interim security clearances kept to a minimum (AR 380-67, para 5-104, and Ft Knox Pamphlet 380-67, para 6-4)?</p> <p>4. Is proper planning exercised to ensure that personnel security investigations are submitted in a timely fashion (AR 380-67, para 5-100, and Ft Knox Pamphlet 380-67, para 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 requests 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. Are subjects notified immediately of required forms to be completed and its urgency stressed as to the expeditious completion of said forms?</p> <p style="padding-left: 20px;">d. Are required forms and prescribed documentation properly executed (Ft Knox Regulation 380-67, para 5-4 through 5-10)?</p> <p>5. Have all personnel engaged in education and orientation duties had a favorable NAC (AR 380-67, para 3-611)?</p> <p>6. Does your annual security education include the Personnel Security Program?</p> <p>7. Are incumbents of critical-sensitive, noncritical sensitive-SECRET, and noncritical sensitive-CONFIDENTIAL positions required to undergo a PR every 5, 10, and 15 years respectively (AR 380-67, para 3-703, Ft Knox Pamphlet 380-67, para 5-6, and 5-10)?</p> <p>8. Is access suspended on individuals failing to complete the required PR within the time prescribed or refusing to complete the forms (AR 380-67, para 5-105c, and Ft Knox Pamphlet 380-67, para 5-12)?</p> <p>9. Is U.S. citizenship verification being completed?</p> <p style="padding-left: 20px;">a. Is citizenship verification accomplished by the S-2/Security Manager (Ft Knox Pamphlet 380-67, para 3-9b)?</p> <p style="padding-left: 20px;">b. Are records maintained which specify who and what document was used to verify an individual's U.S citizenship (Ft Knox Pamphlet 380-67, para 3-9c)?</p> <p>10. Is subject's federal service date without a 24-month break, as defined in AR 380-67, para 1-306.1, verified through official means (Ft Knox Pamphlet 380-67, para 3-7a(1))?</p> <p>11. Are S2/Security Managers ensuring local files checks are not over 60 days old before submission of personnel security actions (Ft Knox Pamphlet 380-67, para 3-7a)?</p> <p>12. Are local file checks properly completed to include unit files for pending unit punishment, records of indebtedness, etc (Ft Knox Pamphlet 380-67, para 3-7a (4))?</p>

INSPECTION CHECKLIST (continued)			
FUNCTIONAL AREA			SUBJECT AREA:
SECURITY			PERSONNEL SECURITY
YES	NO	N/A	INSPECTION ITEM
			<p>GRANTING ACCESS:</p> <ol style="list-style-type: none"> 1. Is access to classified information granted only to individuals whose official duties require such access and who have the appropriate personnel security clearance validated by the local command (AR 380-67, para 7-102, and Ft Knox Pamphlet 380-67, para 6-2)? 2. Is access eligibility withdrawn when no longer required in the normal course of an individual's duties (AR 380-67, para 6-8)? 3. Is an individual's access downgraded when the security clearance is based on an outdated investigation and a request for a PR was not forwarded (AR 380-67, para 7-103, and Ft Knox Pamphlet 380-67, para 5-12)? 4. Are Fort Knox Form 1378s utilized for accepting security clearance/surety determinations on assigned or attached personnel (Ft Knox Pamphlet 380-67, para 6-8)? <ol style="list-style-type: none"> a. Is the degree of clearance/date and type/date of investigation properly extracted from the JPAS screen? b. Are local file checks completed and appropriate annotation made on the form? c. Is the individual signing the Fort Knox Form 1378 the S2/Security Manager? d. Does the Fort Knox Form 1378 reflect current clearance status? 5. Are previously granted clearances only accepted when JPAS or the DCII reflects current clearance and investigation, local file checks are favorable, and there has been no break in Federal Service exceeding 24 months since the investigation date (AR 380-67, para 7-102, and Ft Knox Pamphlet 380-67, para 6-7a)? 6. Is security clearance indicated on TDY orders only after verification is received from the Security Manager? <p>JOINT PERSONNEL ADJUDICATION SYSTEM:</p> <ol style="list-style-type: none"> 1. Have all individuals assigned to your activity been in-processed and owned by the S2/Security Manager in the JPAS Program (Ft Knox Pamphlet 380-67, appendix I)? 2. Have all individuals occupying cleared positions been indoctrinated and access level indicated along with the Non-Disclosure Agreement date been completed in JPAS (Ft Knox Pamphlet 380-67, appendix I)? 3. Has the IT level been indicated in JPAS for all personnel assigned to your activity? 4. Are individuals being out-processed in JPAS when they depart your activity/command (Ft Knox Pamphlet 380-67, appendix I)? 5. Is the S2 Security Manager supplying PSB the names and social security numbers of personnel in/out processing your activity on a regular basis (Ft Knox Pamphlet 380-67, appendix I)? <p>REPORTING OF UNFAVORABLE INFORMATION:</p> <ol style="list-style-type: none"> 1. Is all significant unfavorable information pertaining to assigned or attached personnel being reported using the Incident Report in JPAS (AR 380-67, para 8-101, and Ft Knox Pamphlet 380-67, paras 8-2 and 8-5)? <ol style="list-style-type: none"> a. Are the Incident Reports being properly completed? Is all amplifying information provided to enable an adjudicator to make a thorough and comprehensive security evaluation? b. Are follow-up reports forwarded within 90 days (Ft Knox Pamphlet 380-67, paragraph 8-5a)?

INSPECTION CHECKLIST (continued)			
FUNCTIONAL AREA			SUBJECT AREA:
SECURITY			PERSONNEL SECURITY
YES	NO	N/A	INSPECTION ITEM
			<p>c. Do final reports contain recommendations of the command concerning restoration of the person's access or revocation of his/her security clearance (AR 380-67, para 8-101, and Ft Knox Pamphlet 380-67, para 8-5b)?</p> <p>d. Is PSB furnished a copy of the Incident Report along with any enclosures that were FAXed to CCF (Ft Knox Pamphlet 380-67, para 8-5a)?</p> <p>e. Is the subject notified in writing when access to classified information/SCI has been suspended (Ft Knox Pamphlet 380-67, para 8-15a)?</p> <p>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, paras 8-101 and 8-102, and Ft Knox Pamphlet 380-67, paras 8-2 and 8-14)?</p> <p>a. Are S2 personnel assisting the command by coordinating with the legal clerk for actions such as Article 15, court-martials, suspension of favorable personnel actions, discharge packets, etc? </p> <p>b. Are S2 personnel coordinating with the unit drug/alcohol representative when information is required on drug/alcohol program enrollment/status?</p> <p>CONTINUING SECURITY RESPONSIBILITIES:</p> <p>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, paras 9-200 and 9-201, and Ft Knox Pamphlet 380-67, para 9-4)?</p> <p>2. Are commanders/supervisors familiar with their responsibilities in matters pertaining to personnel security with respect to personnel under their supervision (AR 380-67, para 9-102, and Ft Knox Pamphlet 380-67, para 9-1)?</p> <p>3. 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, para 9-101, and Ft Knox Pamphlet 380-67, para 9-3)?</p> <p>4. 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, para 9-204)? Execute a Security Termination Briefing, DA Form 2962, or the back side of the SF 312 for individuals retiring, ETSing, resigning from civil service, revocation of a security clearance, or contemplated absence from duty or employment for 60 days or more (AR 380-67, para 9-204, and Ft Knox Pamphlet 380-67, para 9-7).</p> <p>SAFEGUARDING PERSONNEL SECURITY REPORTS AND RECORDS:</p> <p>1. Are personnel security actions stored in a locked container or in a similar protected area (AR 380-67, para 10-103, and Ft Knox Pamphlet 380-67, para 10-2b)?</p> <p>2. Are personnel security reports and records afforded only for the purpose cited in AR 380-67, chapter 10, and to persons whose official duties requires such information (AR 380-67, para 10-100, and Ft Knox Pamphlet 380-67, 10-2)?</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, para 10-104, and Ft Knox Pamphlet 380-67, paras 10-2c and 10-5)?</p>

Appendix B

Items to Include in Supplemental Personnel Security Standing Operating Procedures (SOP)

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/FK Form 1378.
 - (1) Preparation.
 - (2) Maintenance.
 - (3) Disposition.
- h. Security Education.
 - (1) Initial briefing.
 - (2) Refresher briefing.
 - (3) Debriefing.

Fort Knox Pam 380-67 (24 Jul 08)

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

Appendix C

MOS Listing

C-1. Security Clearance Requirements for MOS, MOS-Producing Schools, Functional Areas, and Additional Skill Identifiers.

C-2. Enlisted MOS and MOS-producing schools (references DA Pamphlet 611-21, Military Occupational Classification and Structure; SMARTBOOK, online current as of 22 January 2007; DA Pamphlet 351-4, U.S. Army Formal Schools Catalog; MILPER Message 04-183 AHRC-EPD-C. (09S is an officer candidate and 09W is a warrant officer candidate.)

09L - *SECRET	25B - SECRET/PSSP	35Y - TS/SCI
09S - *SECRET	25C - SECRET	35Z - TS/SCI
09W - *SECRET	25D - TS/SCI	37F - SECRET
13C - SECRET	25E - SECRET	38B - SECRET
13D - *SECRET	25F - SECRET	42A - SECRET
13E - SECRET	25L - SECRET	42F - SECRET
13F - *SECRET	25N - SECRET	46Q - SECRET
13M - *SECRET	25P - SECRET	46R - SECRET
13P - *SECRET	25Q - SECRET	46Z - SECRET
13R - *SECRET	25S - SECRET	56M - SECRET
13W - *SECRET	25T - SECRET	89D - TS/SSBI
13Z - SECRET	25U - SECRET	94A - *SECRET
14E - *SECRET	25W - SECRET	94D - SECRET
14J - *SECRET	25X - SECRET	94E - *SECRET
14M - SECRET	25Y - SECRET	94F - SECRET
14R - SECRET	27D - SECRET	94K - SECRET
14S - *SECRET	27G - SECRET	94L - SECRET
14T - *SECRET	31B - CONF/PRP	94M - SECRET
14Z - SECRET	31D - TS/SSBI	94P - *SECRET
15J - SECRET	31E - CONF	94R - SECRET
15N - SECRET	33W - *TS/SCI	94S - SECRET
15P - SECRET	35F - *TS/SCI	94T - CONF
15Q - SECRET	35G - **TS/SCI	94W - SECRET
15W - SECRET	35H - *TS/SCI	94X - SECRET
18B - SECRET	35K - SECRET	94Y - SECRET
18C - SECRET	35L - TS/SCI	94Z - SECRET
18D - SECRET	35M - *SECRET	96R - SECRET
18E - SECRET	35N - **TS/SCI	98P - *SECRET
18F - SECRET	35P - **TS/SCI	
18X - SECRET	35S - **TS/SCI	
18Z - SECRET	35T - *TS/SCI	
21L - SECRET	35U - SECRET	
21U - SECRET	35W - SECRET	
21Y - SECRET	35X - TS/SCI	

C-3. Warrant officer (references DA Pamphlet 611-21, Military Occupational Classification and Structure; SMARTBOOK, online current as of 22 Jun 05). A minimum of an INTERIM SECRET is required to apply for warrant officer.

311A - TS/SSBI	351Y - TS/SCI	352S - TS/SCI
350F - TS/SCI	352N - TS/SCI	353T - TS/SCI
350G - TS/SCI	352P - TS/SCI	910A - SECRET.PRP
350K - TS/SCI	352Q - TS/SCI	
351L - TS/SCI	352R - TS/SCI	

C-4. Commissioned Officer (references DA Pamphlet 611-21, Military Occupational Classification and Structure; SMARTBOOK , online current as of 22 Jan 07; Commissioned Officer Classification System, 26 Jun 95; and DA Pamphlet 600-3, Commissioned Officer Development and Career Management, 28 Nov 97). A minimum of final SECRET is required before being commissioned and applying for Officers Candidate School (OCS). **Functional areas are the following:**

- a. Aviation Tactical Intelligence (15) - TS/SCI.
- b. Civil Affairs (38) - Eligible for TS.
- c. Military Intelligence (35) - TS/SCI.
- d. Space Operations (40) - TS/SCI.

NOTES:

* 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 OPM and favorable adjudication of NAC CCF prior to ship)

Appendix D
Fort Knox Form 1947 (Local Files
Check)

LOCAL RECORDS CHECK				DATE
For use of this form, see Fort Knox Pam 380-67				
EMILPO/OPF RCDS	MED RCDS	PMO RCDS	INTEL RCDS	UNIT RCDS
TO:		FROM:		
Request a records check on the individual listed below for pertinent adverse or derogatory information (see reverse side for additional guidance). Checks resulting in adverse information will be marked "FOR OFFICIAL USE ONLY" and handled accordingly.				
REASON FOR REQUEST:				
<input type="checkbox"/> Security Clearance/Personnel Security Investigation <input type="checkbox"/> Assignment to Sensitive Position <input type="checkbox"/> Other (Specify) _____				
NAME (LAST, First, Middle):		GRADE/RANK:	SSN:	
ORGANIZATION:				
TYPED NAME, GRADE, TITLE OF SECURITY MANAGER/S2/PHONE NUMBER:			SIGNATURE:	
TO:		FROM:		
Local record check reveals the following: <input type="checkbox"/> No adverse or derogatory information. <input type="checkbox"/> Adverse or derogatory information summarized below. <input type="checkbox"/> No record.				
TYPED NAME, GRADE, TITLE:		SIGNATURE:		DATE:

ADDITIONAL GUIDANCE

If no unfavorable information is found, annotate block accordingly. If unfavorable information or, if unable to obtain a copy of the information, summarize all the facts noted.

- a. Personnel records will be screened for records of punishment, reductions in grade, letters of indebtedness, absence without leave, or other unfavorable information.
- b. Medical records will be screened for indications of mental or emotional instability, drug or alcohol abuse, or any other factors which a U.S. Medical Officer determines may make the person unsuitable to hold a security clearance under AR 380-67.
- c. Military Police and local Intelligence records will be screened 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 of information included in paragraph 2-200, AR 380-67.
- d. Unit records will be screened for letters of indebtedness, pending unit punishment, etc.

Appendix E
Acceptable Documents for Proof of U.S. Citizenship

The following documents are acceptable for proof of U.S. citizenship IAW AR 380-67, appendix B-4d, and paragraph 3-9a, this pamphlet:

a. Birth Certificate.

(1) Delayed birth certificate.

(2) Notice from the registrar that no birth record exists, plus secondary evidence. Secondary evidence may include the below listed documents and should have been created as close to the time of birth as possible:

(3) Baptismal certificate.

(4) Certificate of circumcision.

(5) Hospital birth record.

(6) Affidavits of person having personal knowledge of the birth.

(7) Census record.

(8) School records.

(9) Family bible records.

(10) Newspaper files.

(11) Insurance papers.

b. Certificate of naturalization.

c. Certificate of citizenship issued by INS.

d. Report of birth abroad.

e. Passport.

f. DD Form 1966/5, item 41c, August 1985 edition.

g. DD Form 1966/2, item 29c, Jan 89 edition.

h. CCF computer-generated DA Form 873.

Fort Knox Pam 380-67 (24 Jul 08)

- i. Previous clearance in JPAS.

Samples of Acceptable Documents for Verification of US Citizenship

<p>BIRTH CARD CERTIFICATION KENTUCKY DEPARTMENT FOR HEALTH SERVICES REGISTAR OF VITAL STATISTICS</p>		<p>THIS CERTIFICATION IS A TRUE ABSTRACT OF THE ORIGINAL BIRTH RECORD OF THE PERSON NAMED ON THE REVERSE. WHICH RECORD IS ON FILE WITH AND IN OFFICIAL CUSTODY OF THE STATE REGISTRAR OF VITAL STATISTICS AT FRANKFORT, KENTUCKY.</p> <p>ISSUED UNDER AUTHORITY OF CHAPTER 213 KENTUCKY REVISED STATUTES</p>
<p>BIRTH NUMBER 116-60429839-26 NAME OMAR E. GREENMAN BIRTHDATE 6-11-1926 SEX MALE BIRTHPLACE MANKEN COUNTY KENTUCKY RECORD FILED 1926 DATE ISSUED 10-11-83 CARD NUMBER 0000</p> <p><i>Mar L Greeman</i> MAR L GREEMAN STATE REGISTRAR</p>		

<p>STATE OF MICHIGAN DEPARTMENT OF PUBLIC HEALTH</p>		STATE REG NUMBER
<p>LP 000001 OF</p>		<p>CERTIFICATE OF LIVE BIRTH</p>
4550138		
<p>CHILD - NAME 1 JOHN 2 MIDDLE LEE 3 LAST DON</p>		
<p>SEX 1 MALE 2 FEMALE SINGLE</p>		
<p>PLACE 1 HOSPITAL NAME OR NOT HOSPITAL AND STREET AND NUMBER OUTER DRIVE HOSPITAL 2 CITY, VILLAGE OR TOWNSHIP OF BIRTH LINCOLN PARK 3 COUNTY OF BIRTH WAYNE</p>		
<p>CERTIFICATION 1 SIGNATURE DR. WALTER SMITH 2 CERTIFIER NAME AND TITLE (PRINT BY TYPE) DR. WALTER SMITH 3 REGISTRAR SIGNATURE <i>Jane B. Brital</i> 4 DATE RECEIVED BY LOCAL REGISTRAR AND BY TIME April 6 1901</p>		
<p>MOTHER - MAIDEN NAME 1 MARY LOU JONES 2 SOCIAL SECURITY NUMBER 111-111-3647 3 AGE AT TIME OF THIS BIRTH 22 4 STATE OF BIRTH MICH.</p>		
<p>FATHER - NAME 1 HENRY JOHN DON 2 SOCIAL SECURITY NUMBER 222-333-4786 3 AGE AT TIME OF THIS BIRTH 23 4 STATE OF BIRTH MICH.</p>		
<p>MOPH</p>	<p>I CERTIFY THAT THE PERSONAL INFORMATION PROVIDED ON THIS CERTIFICATE IS CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF. SIGNATURE MARY DON DATE 4-3-1901 RELATION TO CHILD MOTHER</p>	

Certificate of Naturalization N-550 or N-570

Issued by INS to naturalized United States citizens.

Certificate of United States Citizenship N-560

Issued by INS to individuals who derived citizenship through parental naturalization; acquired citizenship at birth abroad through a United States parent or parents; acquired citizenship through application by United States citizen adoptive parents; and who, pursuant to section 341 of the Act, have applied for a certificate of citizenship.

Certification of Birth issued by the Department of State
FS-545

Issued by U.S. embassies and consulates overseas to
United States citizens born abroad.

DEPARTMENT OF STATE
FOREIGN SERVICE OF THE UNITED STATES OF AMERICA
Certification of Birth Abroad
of a Citizen of the United States of America

This is to certify that according to records on file in this Office

was born at _____
on _____ day of _____ 19____

In Witness Whereof, I have hereunto subscribed my hand and placed the seal of the Consular Service of the United States of America at _____
day of _____ 19____

(SEAL) _____ of the United States of America

WARNING: This certificate is not valid if it has been altered in any way whatsoever or if it does not bear the printed seal of the Department of State.

Certification of Birth issued by the Department of State
DS-1350

Issued by the U.S. Department of State to
United States citizens born abroad.

DEPARTMENT OF STATE
WASHINGTON, D.C.
Certification of Birth Abroad
of a Citizen of the United States of America

This is to certify that according to records on file in the Department of State

was born at _____
on _____ day of _____ 19____

In Witness Whereof, I have hereunto subscribed my hand and my name subscribed by the Authentication Officer of the said Department of State

day of _____ 19____

(SEAL) _____ of the United States of America

WARNING: This certificate is not valid if it has been altered in any way whatsoever or if it does not bear the printed seal of the Department of State.

Appendix F
Standard Subject Interview Worksheet

STANDARD SUBJECT INTERVIEW WORKSHEET

NAME: _____ SSN: _____ DATE: _____

1. Introduction.

a. Identify yourself and your position to the subject.

b. State the purpose of the interview - Required by AR 380-67, Personnel Security Regulation, to confirm the accuracy of the information on the Standard Form 86 in order to assist DSS, OPM, and CCF in conducting the investigation and determining subject's suitability for access to TS/SCI information. The sole function of the interview is to obtain information. Determining the relevance of this information or the significance of determining eligibility is done by other officials.

c. While it is necessary to obtain signed Privacy Act Advisement statement, release on the SF 86, explain the four main points of the Privacy Act of 1974: (1) Authority, (2) Principal purposes, (3) Routine uses, and (4) Voluntary nature of disclosure versus effects of not providing requested information.

d. The basis for the interview is the SF 86, and questions should follow the order of the form in most cases. Any questions not addressed below should center on the completeness and accuracy of information provided by the subject. If you receive a positive reaction to any question, explore it to the extent that you are satisfied that no additional information exists that could further enhance an understanding of the incident. Remember to use and answer the six basic interrogatives: Who, what, when, where, why, and how.

2. Standard Questions.

(Item numbers relate to the questions on the SF 86 (Security Clearance Application))

Item 1: Is the name on the application your complete legal name? (Yes/No). Is your date and place of birth as indicated on this form correct? (Yes/No) _____

Item 2: Have you ever been known by any other name, a nickname? (Yes/No). Have you ever had a name change as a result of a court action, marriage, divorce, etc.? (Yes/No) Have you ever used a stage or professional name? (Yes/No) _____

Have there been any changes in the spelling of your name? (Yes/No) Is the spelling the same as on your birth certificate/other documents? (Yes/No) _____

SUBJECT INTERVIEW WORKSHEET CONTINUED

NAME: _____

Item 3: Did your security manager verify your U.S. citizenship by checking your birth certificate, passport, certificate of naturalization, etc.? (Yes/No) Explain "No" answer if security manager stated on DD Form 1879 that one of the documents required to be provided by the subject was used. _____

Item 4: Have you listed all actual places of residence during the last 10 years? (Yes/No) In the last 10 years did you experience any difficulties with neighbors, landlords, roommates, or member of the military with whom you have resided? (Yes/No) Would anyone attempt to discredit you during the course of this investigation? (Yes/No) _____

Item 5: In the last 10 years, were you suspended or expelled from school for any reason? (Yes/No) _____

Item 6: Have all periods of employment been listed for the last 10 years? (Yes/No) Did you include all part-time employment while in school or in the military? (Yes/No) _____

Item 7: Do the references on the combined time period cover the 7-year scope of the investigation? (Yes/No) Are any of your references currently in the military? (Yes/No) If so, ensure rank and unit of assignment is listed. _____

Item 8: Have any/all former spouse(s) been listed? (Yes/No) Obtain full identifying date, including current or last know address. _____

Would your former spouse attempt to discredit you? (Yes/No) Obtain details if answer is Yes. _____

Apart from family members, have you ever co-habited with another person with whom a close relationship exists or existed? (Yes/No) _____

Item 9: Are all members of your immediate family indicated (including guardians, step-parents, foster-parents, brother, sisters, step-brothers, step-sisters, children and in-laws, or others to whom you are bound by affections or obligations)? (Yes/No) _____

Item 10: Is your mother, father, sister, brother, child, current spouse, or someone with whom you have a spouse like relationship a U.S. citizen other than birth, or an alien residing in the U.S.? (Yes/No) Obtain identifying data, including name, age, occupation, address, citizenship, extent of contact, and correspondence with the person. _____

SUBJECT INTERVIEW WORKSHEET CONTINUED

NAME: _____

Item 11: Are all periods of military service covered to include membership in the Reserves or National Guard and attendance at a military academy or ROTC? (Yes/No) _____

Item 12: Do you have any foreign business connections? (Yes/No) Have you ever owned any foreign property, bonds, stocks, or land? (Yes/No) _____

Item 13: Have you ever worked for any foreign government, company, or organization? (Yes/No) _____

Item 14: Have all personal foreign travel within the last 7 years outside the U.S., to include Mexico and Canada, been listed? (Yes/No) If "No," indicate where, when, how long, and for what purpose. In the last 7 years, have you been involved in the black market or other illegal activities? (Yes/No) During that time did you experience any problems with the police, customs, or passport official or had any illnesses while in a foreign country? (Yes/No) _____

Item 15: In the last 7 years, have you been involved in an embarrassing, compromising, or questionable activity while in a foreign country? (Yes/No) _____

Item 16: If married, ask same questions in regards to spouse. _____

Item 17: Have you ever been discharged, other than honorable conditions, from the service? (Yes/No) _____

Item 18: Your Selective Service Record – Are you a male born after December 31st 1959? (Yes/No) _____

Item 19: In the last 7 years, have you been a patient or had consultations with a psychiatrist, psychologist, or psychoanalyst? (Yes/No) (Do not include consultations involving martial, family, or grief that was not violent) _____

Item 20: In the last 7 years, have you had any difficulties with supervisors or co-workers? (Yes/No) In the last 7 years, have you been fired or asked to resign from a job? (Yes/No) In the last 7 years, have you left a job knowing you were going to be terminated for a cause? (Yes/No) Did you receive disciplinary action (such as demotion, transfer, reassignment, etc.,) for a job related to misconduct such as fraud, embezzlement or submitting false claims/travel vouchers/timecards? (Yes/No) _____

SUBJECT INTERVIEW WORKSHEET CONTINUED

NAME: _____

Item 21: Ensure that all unfavorable involvement of subject with law enforcement agencies as an adult or juvenile is covered: Have you ever been charged with or convicted of any felony offense (Include those under the Uniform Code of Military Justice.)? (Yes/No)

Item 22: Have you ever been charged with or convicted of a firearms or explosive offense? (Yes/No) _____

Item 23: Are there currently any charges pending against you for any criminal offenses? (Yes/No) _____

Item 24: Have you ever been charged with or convicted of any offenses related to alcohol or drugs? (Yes/No) _____

Item 25: In the last 7 years, have you been subjected to court martial or other disciplinary proceedings under the Uniform Code of Military Justice to include non-judicial? (Yes/No)

Item 26: In the last 7 years, have you been arrested for, charged with, or convicted of any offense not listed in response to the other questions previously asked, except for minor traffic violations, that were not drug or alcohol related? (Yes/No) In the last 7 years, have you had your drivers' license suspended or revoked? (Yes/No) In the last 7 years have you been charged with malicious mischief offenses? (Yes/No) Were you charged with crimes against the public peace? (Yes/No) Were you charged with any sex-related offenses? (Yes/No) Were you charged with any crimes against persons to include spouse or child abuse? (Yes/No)

Item 27: In the last 7 years or since your 16th birthday, whichever is shorter, have you experimented with or been addicted to any narcotics, barbiturates, hallucinogens, or any dangerous or illegal drugs to include marijuana or hashish, LSD, Speed, etc ? (Yes/No)

Item 28: Have you EVER illegally used a controlled substance while employed as a law enforcement officer, prosecutor, or courtroom official; while possessing a security clearance; or while in a position directly and immediately affecting public safety? (Yes/No)

Item 29: Have you ever been involved with the illegal purchase; manufacture; trafficking; productions; transfer; shipping; receiving; or sale or any narcotic, depressant, stimulant, hallucinogen, or cannabis for your own intended profit or that of another? (Yes/No) _____

SUBJECT INTERVIEW WORKSHEET CONTINUED

NAME: _____

Item 30: In the last 7 years, have you used alcoholic beverage to an excess on a recurring basis? (Yes/No) In the last 7 years, have you had any problems associated with your personal consumption of alcohol including police involvement; concerns by employee or supervisor; embarrassing situations; fights; martial difficulties; and/or referral to medical authority, counselor, or rehabilitative programs? (Yes/No) If there appears to be a drinking problem, obtain details of rate of consumption, behavior patterns, and any unfavorable information associated with drinking:

In the last 7 years, have you refused medical treatment or counseling as a result of your use of alcoholic beverages when so directed by competent authority? (Yes/No)

Item 31, 32, 33, 34, 35, 36, and 37: In the last 7 years, have you had any credit or financial difficulties, to include bad checks, collections, repossessions, delinquent accounts, suits, judgments, bankruptcies, or liens? (Yes/No) _____

In the past 7 years, have you failed to pay and file your Federal or State income taxes when required by law? (Yes/No) _____

In the past 7 years, have you had any debts turned over to a collection agency? (Yes/No) Have you defaulted on any loans, including student loans? (Yes/No) Have you been evicted from a residence or left residence owing money for utilities, rent, or damages? (Yes/No) Have you had any credit cards recalled or canceled due to bad debt? (Yes/No)

In the last 7 years, have you engaged in frequent gambling to the extent that you incurred personal financial hardship or gambling involving large sums of money? (Yes/No)

Item 38 and 39: In the last 7 years, have you been over 180 days delinquent on any debts? (Yes/No) Are you currently 90 days delinquent on any debt(s)? (Yes/No) Do you pay your obligations on time? (Yes/No) _____

Item 40: In the last 7 years, have you been a party to any public record civil court actions not listed elsewhere on this form? (Yes/No) _____

Item 41 and 42: Are you now or have you ever been affiliated with any organization, association, movement, group, or combination of people who participate in or advocate to the violent overthrow of the U.S. Government? (Yes/No) Have you ever demonstrated, either legal or illegal, against the U.S. Government? (Yes/No) _____

SUBJECT INTERVIEW WORKSHEET CONTINUED

NAME: _____

OTHER: Have you ever been the subject of an official inquiry for disclosing classified information when not authorized to do so? (Yes/No) _____

Have you ever been the subject of an inquiry involving the loss or mishandling of classified material assigned to your control? (Yes/No) _____

Have you ever been approached to give or sell any Government classified or unclassified material to persons not authorized to receive it, or engaged in espionage or sabotage against the United States? (Yes/No) _____

Have you ever been approached by agents or representatives of a foreign government to provide any information? (Yes/No) _____

Are there any incidents or circumstances that could make you vulnerable to coercion or blackmail or place you in an embarrassing position where pressure could be bought to bear? (Yes/No) Solicit information on an incident, condition, or fact that might negatively impact on the individual's character, reliability, suitability, trustworthiness, or loyalty. Examples are omission of any material facts, dishonest conduct, etc. _____

Do you consider yourself to be a loyal citizen to the United States of America? (Yes/No)

INTERVIEWED BY: _____

REPORT COMPLETED ON: _____

Appendix G

Designation of Sensitive Positions

G-1. Criteria for Position Sensitivity Designation.

a. The criteria to be applied in designating position sensitivity and the codes reflected on the Civilian Sensitivity Roster under the Special Designation column.

(1) **Code 1:** Non-sensitive – Investigation Required (NACI).

(a) Category III Information Technology (IT-III) positions, for example normal users, power user on individual systems for configurations, with non-privileged level access to ISs and devices.

(b) All other positions not identified below.

(2) **Code 2:** Noncritical-Sensitive – Investigation Required (ANACI/NACLIC).

(a) Access to SECRET or CONFIDENTIAL information.

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

(c) Category II Information Technology (IT-II) positions, for example operating system administration of common applications or enclaves, back-up operators with limited privileged-level access to control, manage, or configure ISs and devices.

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

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

(f) Individuals in the Biological or Chemical Personnel Reliability Programs (PRP) or in controlled Nuclear Duty Positions in the Nuclear Weapons PRP.

(g) Any other position so designated by the head of the component or designee.

(3) **Code 3:** Critical-Sensitive – Investigation Required (SSBI/SSBI-PR).

(a) Access to TOP SECRET information.

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

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

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

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

(f) Duties falling under SAPs.

(g) Category 1 Information Technology (IT-1) for example, System Administrators/ Network Administrators (SAs/NAs) for infrastructure devices, IDSs, routers; SAs/NAs for classified systems and devices with privileged-level access to control, manage, or configure IA tools or devices; individuals ISS, networks, devices, and enclaves.

(h) Individuals in critical Nuclear Duty positions requiring entrance in the Nuclear Weapon Personnel Reliability Program.

(i) Any other position designated by the head of the component or designee.

(4) **Code 4:** Special – Sensitive – Investigation Required (SSBI/SSBI-PR).

(a) Positions that require extraordinary national security implications associated with SCI access.

(b) Positions that require access to unique or uniquely productive intelligence sources or methods vital to the United States security.

(c) Positions that could cause grave damage and/or compromise technologies, plans, or procedures vital to the strategic advantage of the United States.

G-2. Criteria for IT Positions and Application.

a. Three categories have been established for designating computer-related positions: IT-I, IT-II, and IT-III. Specific criteria for assigning positions to one of these categories are as follows:

(1) IT-I – Investigation required (SSBI/SSBI-PR).

(a) Serves as SAs/NAs for infrastructure devices, IDSs, routers; SAs/NAs for classified systems and devices with privileged-level access to control, manage, or configure IA tools, or devices, individuals, networks, devices, and enclaves.

(b) Responsibility for the development and administration of agency computer security programs, including direction and control of risk analysis and /or threat assessment.

(c) Significant involvement in life-critical or installation or higher mission-critical systems.

(d) Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system but with relatively high risk for affecting grave damage at installation or higher level or realizing significant personal gain.

(e) Relatively, high risk assignments associated with or directly involving accounting, disbursement, or authorization for disbursement from systems of dollar amounts of \$10 million per year or greater or two lesser amounts if the activities of the individual are not subject to technical review by higher authority in the IT-1 category to ensure the integrity of the system.

(f) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

(g) Other positions, as designated by the agency head, that involve relatively high risk for effecting grave damage or realizing significant personal gain.

(2) IT-II – Investigation required (NACLC/ANACI).

(a) Operating system administration of common applications or enclaves, back-up operators with limited privileged-level access to control, manage, or configure ISs and devices.

(b) Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the IT-1 category. Other areas of responsibility may include information requiring protection under the Privacy Act of 1974, contracts, accounting disbursement, or authorization for disbursement from systems of dollar amounts of less than \$10 million a year, as well as access to and/or processing of proprietary data. Positions designated by the agency head that involve a degree of access to systems that create a significant potential for damage or personal gain less than that in IT-I positions can be included in this paragraph.

(3) IT-III. All other positions involved in Federal computer activities. Investigation required (ENTNAC, NACLC/NACI).

G-3. Detailed Instructions for Completing SF 52-B (sample form on page G-6).

a. Part A – Requesting Office.

(1) Item 1. Note the action requested and include the sensitivity designation, as well as the security clearance required (i.e., Approval of position sensitivity designation of NCSS 2(A), which dedicates Non-Critical Sensitive SECRET).

(2) Item 2-6. Self explanatory.

b. Part B – For Preparation of SF 52B.

(1) Items 1 and 2. Incumbent's name and SSN should be annotated in pencil. If the position is presently vacant, indicate such.

(2) Items 3-6 should be left blank.

(3) Item 7 should reflect Job Title and Position Description Number. Items 8-10 and 14. Self explanatory. Item 11-13 can be left blank.

(4) Items 15-51. Leave blank.

c. Part C- Reviews and Approvals. Part C will be used by the security manager/S2 to reflect approval of the request.

d. Part D – Remarks by Requesting Office.

(1) Included specific justification for the sensitivity designation to include the specific subparagraph in AR 380-67, paragraph 3-101, that applies. If the position is IT sensitive, justification must include position category, IT-1 or IT-II.

(2) Indicate command code, unit identification number, TDA, and paragraph and line number.

e. Part E- Employee Resignation/Retirement. Leave blank.

f. Part F - Remarks for SF 52-B Leave blank.

G-4. Investigative Requirements. Investigative requirements and the stage of initiation and/or completion of the required investigation before subject's appointment along with exceptions to policy (reference AR 380-67, paragraphs 3-202a and 3-203 through 3-204).

a. Noncritical-Sensitive positions. An ANACI shall be requested and the NAC portion favorable completed before a person is appointed to a noncritical-sensitive position. An NACL or NAC conducted during military or contractor employment may also be used for appointment provided the ANACI has been submitted to OPM and there is no more than 24 months break in service since completion of the investigation.

b. Critical-Sensitive positions. An SSBI shall be favorably completed prior to appointment to critical-sensitive positions.

c. Exceptions.

(1) Noncritical-Sensitive. In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NAC portion of the ANACI if the head of the requesting organization finds the delay in appointment would be harmful to the national security and such finding shall be reduced to writing and made part of the civilian personnel record. In such instances, the position may be filled only after the ANACI has been submitted.

(2) Critical-Sensitive. In an emergency, a critical-sensitive position may be occupied pending completion of the SSBI if the head of the requesting organization finds the delay in appointment would be harmful to the national security and such finding shall be reduced to writing and made a part of the civilian personnel record. In such instances, the position may be filled only when the NAC portion of the SSBI has been completed and favorably adjudicated or a previous valid NACI, NAC, NACLIC, or ENTNAC has been completed with the submission of the SSBI.

(3) For use with the exception G-4c(1) and (2) above, a delay in appointment may be considered harmful to national security if:

(a) Regulatory requirements, mission and essential functions, or responsibilities cannot be met.

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

(4) This policy applies to new appointments and to current incumbents of positions when the sensitivity designation is changed.

Fort Knox Pam 380-67 (24 Jul 08)

Standard Form 52-B
Rev. JUL 1991
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 3

REQUEST FOR PERSONNEL ACTION

PART A -- Requesting Office (Also complete Part B, Items 1, 7-22, 32, 33, 36 and 39.)

1. Actions Requested Approval of position sensitivity designation of NCSS	2. Request Number 92-1
3. For Additional Information Call (Name and Telephone Number) Ms. Jane Doe, 4-5643	4. Proposed Effective Date 08/18/1992
5. Action Requested By (Typed Name, Title, Signature, and Request Date) JOHN R. SMITH, C, Admin Div, G3/DPTM	6. Action Authorized By (Typed Name, Title, Signature, and Concurrence Date) ROBERT J. JONES, Director, G3/DPTM

PART B -- For Preparation of SF 50 (Use only codes in FPM Supplement 292-1. Show all dates in month-day-year order.)

1. Name (Last, First, Middle) LYNN, Barbara S.	2. Social Security Number 111-00-1111	3. Date of Birth	4. Effective Date
FIRST ACTION		SECOND ACTION	
5-A. Code	5-B. Nature of Action	6-A. Code	6-B. Nature of Action
5-C. Code	5-D. Legal Authority	6-C. Code	6-D. Legal Authority
5-E. Code	5-F. Legal Authority	6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number Secretary/Steno P154/67432	15. TO: Position Title and Number
--	-----------------------------------

9. Pay Plan	10. Dist. Code	11. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis	15. Pay Plan	17. Dist. Code	16. Grade or Level	19. Step or Rate	20. Total Salary Award	17. Pay Basis
GS	318	07									
12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay	20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay				

14. Name and Location of Position's Organization Administration Division G3 Directorate of Plans, Training and Mobilization U.S. Army Armor Center Fort Knox, KY 40121	22. Name and Location of Position's Organization
--	--

EMPLOYEE DATA

23. Veterans Preference 1 - None 2 - 5-Point 3 - 10-Point/Disability 4 - 10-Point/Compensable 5 - 10-Point/Other 6 - 10-Point/Compensable/30%	24. Tenure 0 - None 1 - Permanent 2 - Conditional 3 - Indefinite	25. Agency Use	26. Veterans Preference for RIF YES NO
27. FEGLI	28. Annuitant Indicator	29. Pay Rate Determinant	
30. Retirement Plan	31. Service Comp. Date (Leave)	32. Work Schedule	33. Part Time Hours Per Biweekly Pay Period

POSITION DATA

34. Position Occupied 1 - Competitive Service 2 - Excepted Service 3 - SES General 4 - SES Career Reserved	35. FLSA Category E - Exempt N - Nonexempt	36. Appropriation Code	37. Bargaining Unit Status
38. Duty Station Code	39. Duty Station (City -- County -- State or Overseas Location)		

40. Agency Data	41.	42.	43.	44.
45. Educational Level	46. Year Degree Attained	47. Academic Discipline	48. Functional Class	49. Citizenship 1 - USA 8 - Other
				50. Veterans Status
				51. Supervisory Status

PART C - Reviews and Approvals (Not to be used by requesting office.)

1. Office/Function	Initials/Signature	Date	Office/Function	Initials/Signature	Date
A. ATZK NCSS approved		19920814	D.		
B.			E.		
C.			F.		
2. Approval. I certify that the information entered on this form is accurate and that the proposed action is in compliance with statutory and regulatory requirements.				Signature	Approval Date

CONTINUED ON REVERSE SIDE
52-118

OVER

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6239
APD PE v2.00

SF 52-B (Reverse)

PART D -- Remarks by Requesting Office

(Note to Supervisors: Do you know of additional or conflicting reasons for the employee's resignation/retirement? If "YES", please state these facts on a separate sheet and attach to SF 52-B.)

Incumbent is required to type, retrieve, and file classified mobilization plans up to and including SECRET. Incumbent is also the automated information systems administrator which categorizes the position as Category II automated data processing. Paragraph 3-101a (2) (a) and (c), AR 380-67 applies

Command Code: TC, UIC W0UNAO, TDA # 0387, Para 001A, Line 08

Degree of security clearance/date granted: _____

Type of investigation/date completed: _____

PART E -- Employee Resignation/Retirement

PRIVACY ACT STATEMENT

You are requested to furnish a specific reason for your resignation or retirement and a forwarding address. Your reason may be considered in any future decision regarding your re-employment in the Federal service and may also be used to determine your eligibility for unemployment compensation benefits. Your forwarding address will be used primarily to mail you copies of any documents you should have or any pay or compensation to which you are entitled.

regulations with regard to employment of individuals in the Federal service and their records, while section 8506 requires agencies to furnish the specific reason for termination of Federal service to the Secretary of Labor or a State agency in connection with administration of unemployment compensation programs.

The furnishing of this information is voluntary; however, failure to provide it may result in your not receiving: (1) your copies of those documents you should have; (2) pay or other compensation due you; and (3) any unemployment compensation benefits to which you may be entitled.

This information is requested under authority of sections 301, 3301, and 8506 of title 5, U.S. Code. Sections 301 and 3301 authorize OPM and agencies to issue

1. Reason for Resignation/Retirement (NOTE: Your reasons are used in determining possible unemployment benefits. Please be specific and avoid generalizations. Your resignation/retirement is effective at the end of the day -- midnight -- unless you specify otherwise.)

2. Effective Date	3. Your Signature	4. Date Signed	5. Forwarding Address (Number, Street, City, State, Zip Code)
-------------------	-------------------	----------------	---

PART 5 -- Remarks for SF 50

FOR OFFICIAL USE ONLY

Civilian Sensitivity Roster

Activity

Date

<u>PD</u>	<u>NAME</u>	<u>GRADE</u>	<u>SSN</u>	<u>JOB TITLE</u>	<u>POSN SENS</u>	<u>SPEC DES</u>	<u>DTAPV</u>	<u>CLNC</u>	<u>INVEST DT</u>	<u>ACTVY</u>
DM01123	Smith, Joe	GS05	000-00-0000	Supply Clerk	NCSS	2(a)(b)	11-Feb-07	S	10-Feb-07	DPTMS

Position Sensitivity

CS - Critical Sensitive
 CSS- Critical Sensitive Secret
 CSTS - Critical Sensitive - Top Secret
 NCS - Noncritical Sensitive
 NCSS - Noncritical Sensitive Secret
 NCSC - Noncritical Sensitive Confidential

Degree of Clearance

T - Top Secret
 S - Secret
 C - Confidential
 I - Interim
 N - None
 P - Pending

Investigation Type

A - SSBI
 B - SSBI/PR
 C - NACI
 D - ANACI
 E - Exception to Policy
 F - Secret/PR
 O - Other

Explanation of Headings:

PD - Position Description Number or Job Description Number

NAME - Employee Name

GRADE - Pay Grade of Employee (Example: GS11, YA2)

SSN - Social Security Number

JOB TITLE - Secretary, Security Assistant etc.

POSN SENS - Definition is Position Sensitivity (Example: NCS, NCSS etc) criteria can be found in Appendix G-1

SPEC DES - Definition is Special Designation (Example: 2(a)(b) Criteria can be found at Appendix G-1

DTAPV - Date the position was approved from SF52, Part C

CLNC - Type of Clearance (Example: Secret, Top Secret etc. Individual may be in a NCS position which does not require a clearance, in this case put N for None.

INVEST - Date investigation was closed or submitted

ACTVY - Name of your organization

FOR OFFICIAL USE ONLY

**Appendix H
Request for Exception to Policy to Hire**

Interim Clearance Required

LETTERHEAD IF NEEDED

OFFICE SYMBOL

Date

MEMORANDUM FOR Security Division, DPTMS (OFFICE SYMBOL)

SUBJECT: Request for Exception to Policy to Hire – NAME, SSN

1. Exception to policy is requested regarding the hire of (SELECTEE NAME), Position Title: _____, sensitivity designation approval number ____.
2. (SELECTEE NAME) has been recruited and selected to fill the _____ position, which is a Noncritical-Sensitive-SECRET (NCSS) position. An exception to policy is required to hire, because (SELECTEE NAME) does not currently have the required investigation. It is imperative that (SELECTEE NAME) occupy the position in order to maintain the mission momentum for this office.
3. Duties will require the selectee have access to classified material. Request an interim clearance be granted to enable (SELECTEE NAME) to perform his/her daily duties.
4. Point of contact is _____, Security Manager, (activity), 4-_____.

SIGNATURE BLOCK

FOR OFFICIAL USE ONLY

No Interim Clearance Required

LETTERHEAD IF NEEDED

OFFICE SYMBOL

Date

MEMORANDUM FOR Security Division, DPTMS (OFFICE SYMBOL)

SUBJECT: Request for Exception to Policy to Hire – NAME, SSN

1. Exception to policy is requested regarding the hire of (SELECTEE NAME), Position Title: _____, sensitivity designation approval number ____.
2. (SELECTEE NAME) has been recruited and selected to fill the _____ position, which is a Noncritical-Sensitive-SECRET (NCSS) position. An exception to policy is required to hire, because (SELECTEE NAME) presently does not have the required investigation. It is imperative that (SELECTEE NAME) occupy the position in order to maintain the mission momentum for this office.
3. Although duties will require (SELECTEE NAME) to have access to classified material, there is sufficient work of an unclassified nature to keep him/her gainfully employed pending the issue and receipt of a security clearance. Selectee's supervisor will ensure he/she has no access to classified material until notification is received that a clearance and access have been granted.
4. Point of contact is _____, Security Manager, (activity), 4-_____.

SIGNATURE BLOCK

FOR OFFICIAL USE ONLY

Previous Valid Clearance

LETTERHEAD IF NEEDED

OFFICE SYMBOL

Date

FOR Security Division, DPTMS (OFFICE SYMBOL)

SUBJECT: Request for Exception to Policy to Hire – (NAME)

1. Exception to policy is requested regarding the hire of (SELECTEE NAME), Position Title: _____, sensitivity designation approval number ____.
2. (SELECTEE NAME) has been recruited and selected to fill the _____ position, which is a Noncritical-Sensitive-SECRET (NCSS) position. An exception to policy is required to hire, because (SELECTEE NAME) presently does not have the required investigation. It is imperative that he/she occupy the position in order to maintain the mission momentum for this office.
3. The duties will require (SELECTEE NAME) to have access to classified material. He/She has a current clearance and less than a 2-year break in service. Clearance will be valid upon submission of the required investigation based on Fort Knox Pam 380-67, Chapter 4, paragraph 4-7b3.
4. Point of contact is _____, Security Manager, (activity), 4-_____.

SIGNATURE BLOCK

FOR OFFICIAL USE ONLY

Noncritical Sensitive, No Clearance Required

LETTERHEAD IF NEEDED

OFFICE SYMBOL

Date

MEMORANDUM FOR Security Division, DPTMS (OFFICE SYMBOL)

SUBJECT: Request for Exception to Policy to Hire – NAME, SSN

1. Exception to policy is requested regarding the hire of (SELECTEE NAME), Position Title: _____, sensitivity designation approval number __.
2. (SELECTEE NAME) has been recruited and selected to fill the _____ position, which is a Noncritical-Sensitive (NCS) position. An exception to policy is required to hire, because he/she presently does not have the required investigation. It is imperative that (SELECTEE NAME) occupy the position in order to maintain the mission momentum for this office.
3. Point of contact is _____, Security Manager, (activity), 4-_____.

SIGNATURE BLOCK

FOR OFFICIAL USE ONLY

Appendix I Joint Personnel Adjudication System (JPAS) Instructions

I-1. NEVER use the back button on the web page; it will lock you out of JPAS. To log out, you must click on the log out button in the left column. If you type the wrong password three times, you are locked out of the system. You must call 502-624-6741 or 502-624-2418 to log you out of JPAS. If you accidentally click the back button, you can wait until after midnight, and the system will reset and let you log in again. The system automatically times you out; that is not a lock out, just log in again.

I-2. Computer Requirement. You can access JPAS through Internet Explorer. Your IMO must load the firewall client for the ISA server to access JPAS if you cannot access JPAS.

I-3. Internet Site. <https://jpas.dsis.dod.mil/>.

I-4. Getting Started. Enter internet site, >JPAS Login> agree> enter user id (all lower case)> enter password> log in> okay.

I-5. Select Person. You must enter a SSN to query the system.

I-6. Actions Required on Each Individual. Everyone that belongs to your organization, regardless if they have a security clearance or not, should be in-processed into JPAS; everyone in your organization will be owned. Before you take any action on the individual in JPAS, such as requesting a clearance, reporting derogatory information, or sending a visit request, you must in-process the individual. Only one security management office (SMO) can own a person at a time per category; if a previous unit owned the individual, we are unable to own that person. If there is a telephone number beside the Non-SCI SMO (this is located under person category), call the previous unit and request them to out-process the individual; if not, all we can do is indicate servicing instead of owning. If they have access to classified information, you must indoctrinate them by indicating the date the Nondisclosure Agreement was signed access level, and indicate the IT level. Out-process when the individual departs this command. If you have granted the individual access, you must debrief the individual in the Debrief column. These procedures are explained below.

I-7. Person Summary. This column includes: Open Investigation, PSQ Sent, NDA Signed, Request to Research/Upgrade Eligibility.

I-8. PSQ Sent. Enter the date when you submit an investigation to OPM.

I-9. Non-SCI Access History. This is the history of access granted by other security manager offices.

I-10. Request to Research/Recertify Upgrade Eligibility. This has replaced the DA Form 5247-R. Use this form when the investigation has been closed for over 18 months and the clearance has never been issued or to correct the ORB/ERB. CCF is currently over a year backlogged on issuing clearance for closed investigations. We will no longer be required to

request a clearance from CCF on someone whose investigation was submitted by a previous unit. By owning the individual, CCF will know to send the clearance notification to this installation. How to use Request to Research/Recertify Upgrade Eligibility. Under justification, you must always include what document was used to verify citizenship and the federal service date without a 2-year break in service. Always include your name and telephone number (use your commercial number) in the remarks section. Indicate adjudication type> select CAF – Army CCF >and then print screen before you save it. When you click save, the request goes directly to CCF. Send this office a copy of the form you printed for our records. If an INTERIM SECRET is required, you will submit a DA Form 5247-R to this office.

I-11. Accesses. This column contains: Category, PSP (clearance granted) IT level, Indoctrinate Non-SCI, Grant Interim, and Debrief. **Before you can enter any of these fields, you must in-process through JPAS.**

I-12. Indoctrinate Non-SCI. You must enter the date the Nondisclosure Agreement (NDA) was signed. You have to enter this information before you can indicate the type of access in JPAS. This is a one-time action; you cannot change this information unless you debrief the individual. Access level is indicated in this block. After indicating the NDA date, you need to add the access level date (this is the day you created your FK Form 1378) > save. Indicate IT level.

I-13. PSP. The correct clearance level must be indicated in this block, or you cannot grant access to the individual. This is the access block used by other security managers to grant access. JPAS has replaced visit request.

I-14. Debrief. When an individual no longer requires access to classified information or he/she departs your command, you need to debrief him/her in the JPAS before you out-process him/her. Enter today's date > save. (This does not mean execute a DA Form 2962 or the bottom back side of the SF312. If the individual stays in this service, do not execute either one of these forms.)

I-15. Grant Interim. Security Division will input the interim clearance upon issuance of an Interim, if applicable.

I-16. Person Category Information. This column contains the following: Report Incident, In/Out Process, Suspense Data, and Investigation Request.

I-17. In-process. Click on In-process > add new relationship> enter date (you cannot back-date; you must use today's date) > check owing > click save. Before you in-process, ensure the correct category is marked under "Person Category" on the individual; some people are in the military and contractor or civil service at the same time. Own the person under the correct category. Do not own Reserve Soldiers who are currently mobilized, which includes Individual Ready Reserves (IRR), Individual Mobilization Augmentees (IMA), Retirees and Regional Readiness Reserve Commands (RRCs) and Training Divisions (TDs). Only service these individuals. Be sure to send the Personnel Security Branch a list of those who have in-processed/out-processed your activity. This list should contain the name and SSN.

I-18. Out-process. If individuals were indoctrinated, they must be debriefed before you out-process them. Enter the out date and then save.

I-19. Civilian Employee/Active Duty Army. “Office Phone Comm,” you should add the commercial telephone number and “Office Phone DSN,” add your DSN number. In “Office Symbol,” enter your office symbol.

I-20. Report Incident. This has replaced the DA Form 5248-R. Mark initial, follow-up, or final>date of incident>Select CAF (Army CCF)>Indicate incident criteria >. You can reference the MP blotter and explain the incident as written on the MP blotter. You may also include any commander recommendations along with your name, title, and contact number (use your commercial number) in the incident report. Prior to clicking the save button, print the form you just created. After you click save, it goes directly to CCF. To print after you have sent the form, go into report incident, click on select existing incident drop down tab, and then you can print the last report that comes up (If it was a final report, you cannot print it after you have sent it to CCF.) Any enclosures (MP blotter if referenced) will have to be forwarded to CCF via fax 301-677-2706, DSN 622-2706, or e-mailed to INCIDENTREPORT@CCF1.ftmeade.army.mil. Pay close attention to detail when completing the report incident and follow the instructions in Fort Knox Pamphlet 380-67, chapter 8. Always give who, what, when, where, and how action was taken. Remember, you will still have to follow-up these reports to CCF every 90 days. Each time you send a report, forward a copy of the form you sent to CCF along with any enclosures to Security Division, DPTMS.

I-21. Submit Investigation. Select person> Person Category highlight Investigation Request>Eligibility is whatever clearance is needed>. Do not use the override justification button; we do not have that authority. Next screen will show Local Agency Check date LFC were conducted> Access Code fill in either Secret or Top Secret> ADP mark ADP III unless the individual occupies a I or II position>SON #A054>OPAC-ALC – Use your MACOM (TRADOC is DA-TRAD) and (IMCOM is DA-IMA)>. Security Folder, indicate NPI unless we have a derogatory files check results, then fill in with our address> Military indicate Personnel Services Address (Bldg. No. 1384, One Stop (IMSE-KNX-HRM), Room 103, 58 Vine Grove Rd, Fort Knox, KY 40121-5102 and civilians indicate Civilian Personnel Advisory Center (301 Marshall Avenue, Fort Riley, KS 66442-7005). After completing the required fields, initiate the PSI. Give subject of the investigation a copy of the Subject’s e-QIP Quick Reference to follow.

a. After subject notifies the security manager that they have certified the SF 86, the security manager will have to wait 24 hours after certification and then go into Add/Modify Investigation Request and review and certify the investigation.

b. Before the investigation can be reviewed and approved, the signed SF 86 Certification Form and Information Release Form and the Medical Form (if Item 21 was answered yes) must be forwarded in JPAS. The forms can be scanned or faxed in JPAS. Each form will have to be scanned individually and identified (Example: (SF 86 Certification (Smith)) (Release (Smith))). Go to Document History under the Investigation Request Documents Ready for Review, Go to Document Upload and attach the form that you scanned and saved on your computer. If you fax,

you will fax to 1-855-804-0686. After the scanned releases or faxed releases are received, you will be able to review and approve.

c. After selecting the Approve Button, provide Security Division, DPTMS, the Add/Modify notification indicating the PSQ was sent and the fingerprint charts, if required. This office will forward fingerprint charts to OPM.

I-22. Create/Modify Visit. First thing you have to do is obtain the SMO from the S2/security manager that you are sending the visit request to. Select Create/Modify Visit>add visit>complete visit request information<select SMO>search>click on SMO code>save>add visitor>type SSN>search>check the add block>add>cancel<permanent certification>save <cancel<open visit SMO name>print page for your records. Remove the visit request from the system when no longer needed. The visit request has been sent to the S2/security manager.

I-23. Investigation Summary. "Investigation History." This contains the history of the investigation. If a No Record shows up in investigation block, contact 624-6741/624-2418, to conduct a DCII to check on an investigation. If access is required, ensure the investigation is not over 5 years old for a TOP SECRET, 10 years old for a SECRET, and 15 years old for a CONFIDENTIAL. The clearance remains valid if JPAS reflects the appropriate investigation has been submitted to OPM or is open at OPM.

I-24. Adjudication Summary. "Adjudicative History" indicates the adjudication conducted by CCF and shows where a clearance has been granted by CCF.

I-25. External Interfaces. "Perform SII Search." This goes into the OPM data base and reflects the investigation status at OPM. The DCII is not working in JPAS unless you have permission from this office to conduct a DCII.

I-26. PSM Net. You can own all of the people assigned to your activity in one action without adding them individually but will still be required to indoctrinate them individually. Click on PSM Net > Mark Person Categories by Organization> Add>Mark Owing and Select organization> Change category to Army and type your UIC in the box (Organization, UIC/RCU/PASCODE/CADE)>Search>click on the UIC in purple>OK>Search>Check beside each name you want to add. Add at the end of each page to save the changes made.

I-27. Adding An Individual to JPAS. For military or federal civilian personnel not listed on JPAS who have been in the service for more than 4 weeks, use the Test Problem Report (TRP) form found on the log in screen on JPAS to report a "data" problem. The "Problem Title" should be "Record Not Found in JPAS." Include the following information in the "Detailed Description" block: Subject's full name, SSN, DOB, and affiliation (e.g. Active Army, Reserve, Civilian, etc). To add a contractor or new civilian employee for initiation and submission of an e-QIP investigation perform the following actions: Click on Select Person>Enter the person's SSN>Click the Display Add/Modify Non-DoD Person Radio button> Click the Display button>The Add/Modify Non-DoD Person screen will appear>Enter all the information on the person in the blank fields, with the exception of Date of Death, Cadency, Martial Status, and AKA. The category for new civilian employees will be added as "Seasonal Employee." The

category for new contract employees will be added as "Industry." See instructions for work-around in appendix K of this pamphlet.

I-28. JPAS Access. To obtain access to JPAS, you must go to your account manager. Your account manager for Fort Knox is the Chief, Personnel Security Division Branch, or personnel security assistants. You cannot have access to JPAS if your SECRET clearance is based on a NAC or ENTNAC; it must be a NACLIC, ANACI, SECRET/PR, SSBI, or PR.

I-29. FUTURE. The JPAS system has replaced the issuance of Security Clearance, DA Form 873. CCF will notify the security office when a clearance is granted by Eligibility Change Notification; this notification will stay on the system for 15 days. SCI access will be on the JPAS, and SCI access will not have to be passed from installation to installation. JPAS has replaced the DA Form 5248-R and DA Form 5247-R.

This is not a total run down of JPAS, but it will assist in areas that you are required to input information. The Desktop Resource for JPAS is a guide you should have on hand to assist you in JPAS.

(This page intentionally left blank)

Appendix J Subject's e-QIP Quick Reference

J-1. Starting the SF 86. After initial request has been submitted to e-QIP by the security manager/S2, you will have 30 days to start the investigation and 90 days to complete it. If the 30 days or 90 days elapses, the investigation must be canceled and then resumed by the security manager.

J-2. Working Copy SF 86. You can obtain a working copy of the SF 86 at <http://www.opm.gov/forms/html/sf.asp> to fill out prior to starting in e-QIP.

J-3. e-QIP Website. You must go to e-QIP at www.opm.gov/e-QIP/ to start the investigation after your security manager instructs you to complete the SF 86. You will be provided the Applicant Electronic Questionnaires for Investigations Processing (e-QIP) Handbook by your security manager/S2. Most computers will not go to the site because of the TLS 1.0 setting. After you log into Applicant site and select continue, read how to set the TLS 1.0.

J-4. Three Golden Questions. You will have to type in the answers to the 3 Golden Questions: (1) What is your LAST NAME? (2) In what CITY were you born? (**unknown** must be entered) (3) In what four-digit YEAR were you born? (Example 1963). After these questions are answered, you will proceed to 3 more Golden Questions that no one else will know. Place an "X" in the box to allow you to see your Golden Questions (**THIS IS VERY IMPORTANT, because you cannot go back into the questionnaire if you forget the 3 Golden Question answers. Use something that will not change, for example: eye color or child's name**). The best way to check the 3 Golden Questions is to review the answers after they are typed in to make sure everything is spelled correctly. If answers to the 3 Golden Questions are forgotten and you type in 3 wrong answers, e-QIP will lock you out. You will have to notify the security manager to re-start the investigation.

J-5. Correct Answers. After entering these questions, your name, along with "unknown" and "state," will be reflected on the screen wanting to know if this is correct. This is correct.

J-6. Do not Use the Forward or Back Button. Do not use the forward or back button in e-QIP. Tab to next screen, and use the mouse or keyboard to navigate the e-QIP screen and Tab key to move between links and other from controls. Click save or continue at the bottom of each screen (if the screen has not validated, the system will tell you what needs to be corrected). To go from one screen to another, go to navigate top of screen, enter module you want to go to and select go.

J-7. Country. When entering addresses, do not enter a country if state is typed in the Address block; only enter country if other than U.S. Use the look up list in e-QIP; you will need to copy and paste. Leave the list open until you exit e-QIP.

J-8. References. Each residence and employment will require a reference.

J-9. Charter References. Charter references are required for 5-year time periods only.

J-10. ZIP Codes. You are required to enter a zip code for all states in the U.S. There is no zip code requirement for all other countries. Go to www.usps.com to locate a zip code.

J-11. Selective Service Number. Selective service number is required. Go to www.sss.gov to obtain the number.

J-12. Validation. After completion of the SF 86, you will need to validate the form to ensure there are no errors.

J-13. Certify. Prior to certifying, a working copy of the form needs to be printed and reviewed by the security officer (go to display >file>print start at page 5). After reviewing, the form is ready for certification. Follow the directions after certification. Print an Archival Copy of the form Pages 1, and 6 forward (2-5 is the privacy information). Print the signature pages and give a copy of the printed forms with the signed pages to the security manager. If errors are found after certification, the SF 86 will have to be revised and resumed through JPAS by the security manager/S2 so the errors can be corrected. Answers to questions 21-30 will be blank and will have to answered again. It is suggested that you save a copy of the questionnaire to your computer or a diskette.

J-14. Release Request/Transmit to Agency. Finally the "Release Request/Transmit to Agency" link will be selected (After selecting the release, you will no longer have access to the form). This sends the application to the Security Manager.

Appendix K
Electronic Questionnaires for Investigations Processing (e-QIP)

K-1. Security Manager's e-QIP Quick Reference.

a. Initiate Investigation. Security manager/S-2 must submit request for investigation through JPAS. You must own or service an individual before requesting an investigation. You also must be granted authorization to initiate investigation (this is accomplished by the account manager).

b. Manage Investigation Request. You will be able to see the status of an investigation by looking at the Manage Investigation Requests in JPAS.

c. Time Frame to Start Investigation. After initial request has been submitted, subject has 30 days to start the investigation and 90 days to complete it. If the 30 or 90 days elapses, the investigation must be cancelled by selecting the Stop Request Button in JPAS, selecting SAVE, and then Resume Request Button in JPAS.

d. E-QIP Web Page. Subject must go to E-QIP at www.opm.gov/e-QIP/ to start the investigation after initiating the investigation in JPAS. Provide the subject a copy of the Subject's e-QIP Quick Reference, along with the Applicant Electronic Questionnaires for Investigations Processing (e-QIP) Handbook, DA, October 2006, when instructing use of e-QIP.

e. Three Golden Questions. Subject will have to type in the answers to the following 3 Golden Questions:

- (1) What is your LAST NAME ?
- (2) In what CITY were you born? (**unknown must be entered**)
- (3) In what four-digit YEAR were you born? Example 1963.

After these questions are answered he/she can go into 3 more Golden Questions that no one else will know (**THIS IS VERY IMPORTANT, SUBJECT cannot go back into the questionnaire if he/she forgets the 3 Golden Question Answers**). The best way to check the 3 Golden Questions is to review the answers after they are typed in to ensure everything is spelled correctly. If answers to the 3 Golden Questions are forgotten, you will have to Stop Request in JPAS and then Resume Request in JPAS. When Stop is used, there will be three new Golden Questions for the subject to answer. Subject has three chances to enter the correct answer; if incorrect answers are entered three times, the subject will be timed out. You will have to Stop Request and then Resume (usually the subject cannot go into e-QIP until the next day).

f. Do not Use Forward or Back Button. Do not use the forward or back button in e-QIP. Tab to next screen.

g. Review Subject's SF 86. After subject completes the SF 86, he/she will need to validate it to be sure there are no errors. He/She will save at the end of each screen. Prior to certifying, a working copy of the form needs to be printed and reviewed by the security officer. After review, subject can certify the form. If errors are found after certification, the SF 86 will have to be Revised through JPAS so subject can correct the errors (When revised has been indicated, questions 21-30 will have to be answered again by the subject). If the form is correct after certifying, the subject will print the forms by selecting the "DISPLAY the Archival Copy of the investigation and request printing" and "Display the Signature Forms for printing links." It is suggested the subject save a copy of the questionnaire to his/her computer or diskette.

h. Subject Releases/Transmit. Finally, the "Release Request/Transmit to Agency" link will be selected (After selecting the release, subject will no longer have access to the form.)

i. Wait 24 Hours. After subject notifies the security manager that he/she has certified the SF 86, the security manager will have to wait 24 hours after certification and then continue processing the investigation. If you do not receive the e-QIP forms for release after 24 hours of release by the subject, you will need to stop PSQ, save, wait 2 hours, and resume PSQ. Wait 24 hours, and the PSQ status should change to ready for review.

j. Scan Releases. Before the investigation can be reviewed and approved, the signed SF 86 Certification Form and the Information Release Form and the Medical Form (if Item 21 was answered yes) must be forwarded in JPAS. The forms can be scanned or faxed in JPAS; this is the preferred method (The investigation opens quicker with the scanned releases.) Each form will have to be scanned individually and identified, Example: (SF 86 Certification (Smith)) (Release (Smith)). Go to Document History under the Investigation Request Documents Ready for Review, Go to Document Upload, and attach the form you scanned and saved on your computer.

k. FAX Releases: Fax to 1-866-804-0686. A few rules to follow when faxing:

(1) DO.

(a) Print out the release forms from the subject's e-QIP submission. Certification of SF 86 (CER), Authorization for Release of Information (REL) and Authorization for Release of Medical Information (MEL) (if required).

(b) Have subject sign and date the forms.

(c) Fax all three forms in the same transmission.

(2) DO NOT.

(a) Send a fax cover sheet.

(b) Do not send anything other than the signed release forms. Do not send in previous editions of release forms and do not send any additional correspondences.

(c) Do not write additional information on the signature forms. The only additions to the form will be the Subject's signature and date. In the event this is a PR/Secret PR investigation, also include the statement "Periodic Reinvestigation Fingerprints are not required" in the "Other Names Used" block.

(d) Do not send a fax...fax only the original signed release form. Double and triple faxed forms cannot be read by the OCR.

(e) Do not forget to date the forms. Forms without numbers will be rejected by OPM.

(f) Do not use a fax machine that adds streaks, lines, or other marks on the fax. If your incoming faxes are blurred or contain extraneous marks/lines, do not use that fax to fax in your release forms.

(g) Do not use the originally-signed release forms if you revised the PSQ. A revised PSQ will have a new ID number, and the release forms must have the same ID number.

(h) Do not send a fax that is crumbled, edges folded, or is unreadable.

l. Ready for Review/Approval. After the scanned releases or faxed releases are received, you will then be able to review and approve in JPAS.

m. Approve. After selecting the Approve Button, go into the SII in JPAS and perform a search to see if the investigation has been received. This usually occurs the next day.

n. PSQ Sent. In JPAS, you need to indicate the investigation has been sent. Go into the PSQ sent and complete the blocks in their entirety.

o. Add/Modify Notification. After selecting the Approve Button, provide this office a copy of the Add/Modify Notification indicating the PSQ was sent. Remember to forward the fingerprint charts to this office for submission. In the Reason for Fingerprint, indicate the e-QIP Investigation Request Number. OPM normally opens the investigation within 2 to 3 weeks of approval and release. However, the investigation will not be opened until they receive the fingerprint cards.

p. Check Notification. Check your notification after a month to see if the investigation has opened. If not opened, conduct a SII Search to see why it was not opened. If you have questions, you may call this office or the Help Desk at 888-282-7682, or e-mail occ.cust.serv@dss.mil.

K-2. e-QIP/JPAS Work-Arounds. For those cases where new civilian hires, civilian applicants, and ROTC cadets are not reflected within JCAVS, you will have to manually establish the profile in JCAVS using the "Add/Modify Non DOD" radio button, as noted below in "How to Add a Record".

K-3. How to Add a Record.

a. Introduction. When you attempt to “look up” a person’s record in JCAVS and receive an error message the person does not exist, there is no record within JPAS for that person. **Make sure you have entered the correct SSN.** If you are sure you entered the correct SSN and still receive the error message that the person does not exist, you will have to create a record within JPAS for this person.

b. Instructions.

- (1) Log in as a **User**.
- (2) Click on **Select Person** (column on left).
- (3) Enter the person’s **SSN**.
- (4) Click the **Display Add/Modify Non-DoD Person** radio button.
- (5) Click the gray **Display** button.
- (6) The **Add/Modify Non-DoD Person** screen will appear.
- (7) Enter all the information on the person in the blank fields with the exception of Date of Death, Cadency, Marital Status, and AKA.
- (8) Select **Seasonal Employee** under the **Available Category Types** and then **click** on **“Add Category”**. It will automatically populate the category as Seasonal Employee. You will not need to enter a separation date but will need to click on “Not Applicable” in the **Separation Code** drop down box.
- (9) Click the gray **Save** button to save personal identifying data (PID) information.
- (10) **Determine Investigation Scope Screen.** Select the type of Eligibility using the drop down box required for the investigation request. Click on the gray **Determine Investigation Type**.
- (11) **Initiation Scope.** The Duty Position Code must be left blank.
- (12) Once the subject has been established in JCAVS, you can initiate e-QIP.
- (13) Once the personnel information flows into JCAVS and the correct person category is reflected, you will take ownership of the “Civilian or ROTC Cadet” category. After 24 months of inactivity on the “Seasonal Employee” category, the record will be archived.
- (14) Please do not hesitate to contact the Defense Security Service (DSS) Help Desk at 1-888-282-7682 when you have JPAS, e-QIP, or DCII questions.

**Appendix L
Fingerprint**

Appendix L APPLICANT		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK						FBI		LEAVE BLANK			
SIGNATURE OF PERSON FINGERPRINTED (SIGNATURE OF PERSON FINGERPRINTED)		RESIDENCE OF PERSON FINGERPRINTED		LAST NAME NAM		FIRST NAME		MIDDLE NAME		LAST		FIRST		MIDDLE	
DATE		SIGNATURE OF OFFICIAL TAKING FINGERPRINTS (SIGNATURE OF OFFICIAL)		ALIASES AKA		List all aliases Last, First, Middle		USDIS000Z		DATE OF BIRTH DOB		Month Day Year		PLACE OF BIRTH POB	
EMPLOYER AND ADDRESS Employer Name Employer Address		REASON FINGERPRINTED Reason Fingerprinted		FINGERPRINT QIA		FINGERPRINT QIA		(See below for Codes)		City, State or		Foreign Country			
EMPLOYER AND ADDRESS Employer Name Employer Address		REASON FINGERPRINTED Reason Fingerprinted		FINGERPRINT QIA		FINGERPRINT QIA		(See below for Codes)		City, State or		Foreign Country			
EMPLOYER AND ADDRESS Employer Name Employer Address		REASON FINGERPRINTED Reason Fingerprinted		FINGERPRINT QIA		FINGERPRINT QIA		(See below for Codes)		City, State or		Foreign Country			
EMPLOYER AND ADDRESS Employer Name Employer Address		REASON FINGERPRINTED Reason Fingerprinted		FINGERPRINT QIA		FINGERPRINT QIA		(See below for Codes)		City, State or		Foreign Country			
EMPLOYER AND ADDRESS Employer Name Employer Address		REASON FINGERPRINTED Reason Fingerprinted		FINGERPRINT QIA		FINGERPRINT QIA		(See below for Codes)		City, State or		Foreign Country			
EMPLOYER AND ADDRESS Employer Name Employer Address		REASON FINGERPRINTED Reason Fingerprinted		FINGERPRINT QIA		FINGERPRINT QIA		(See below for Codes)		City, State or		Foreign Country			

ALL FINGERS MUST BE ACCOUNTED FOR. ANNOTATE ANY AMPUTATIONS OR BANDAGES.

WEIGHT Whole Pounds Only If weight is unknown - enter 000 If weight is in excess of 499 - enter 499	SEX Male - M Female - F	HEIGHT Whole Inches Only If entering inches only - Ex. 5ft 11in - 71" If entering feet and inches - Ex. 5ft 11in - 5'11"
--	-------------------------------	---

If Subject Is	(Predominant Race)	Enter Code	Eye Color	Code	Hair Color	Code
Chinese, Japanese, Filipino, Korean, Polynesian, Indian, Indonesian, Asian Indian, Samoan, or any other Pacific Islander		A	Black	BLK	Black	BLK
A person having origins in any of the black racial groups of Africa		B	Blue	BLU	Black	BLK
American Indian, Eskimo, or Alaskan native, or a person having origins in any of the 48 contiguous states of the United States or Alaska who maintains cultural identification through tribal affiliation or community recognition		I	Brown	BRO	Blond or Strawberry	BLN
Of indeterminate race		U	Gray	GRY	Brown	BRO
Caucasian, Mexican, Puerto Rican, Cuban, Central or South American, or other Spanish culture or origin, regardless of race		W	Green	GRN	Gray or Partially Gray	GRY
			Hazel	HAZ	Red or Auburn	RED
			Maroon	MAR	Sandy	SDY
			Multi-Colored	MUL	White	WHI
			Pink	PNK	Unknown	XXX
			Unknown	XXX	Blue	BLU
					Green	GRN
					Orange	ONG
					Pink	PNK
					Purple	PLE

SAMPLE FINGERPRINT CARD

(This page intentionally left blank)

(This page intentionally left blank)

Appendix N
Instructions for Completion of FK Form 1378

Items 1-3, 5, and 6. Self-explanatory. This information should agree with information noted in JPAS pertaining to subject.

Item 4. Self-explanatory.

Item 8. Indicate military unit of assignment, if applicable.

Item 9. Self-explanatory.

Item 10. Information to complete this block is extracted from Civilian Position Sensitivity Report.

Item 11. Information is extracted from JPAS in the Adjudication Summary Block.

Item 12. Indicate the level of access to classified information is authorized.

Item 13. Date the SF 312 was executed.

Item 14. Information is extracted from JPAS in the Investigation Summary Block.

Item 15. Indicate type of Special Access Programs the individual is read into.

Item 16. Annotate the numbers the files checks were completed. Finance Records are no longer available.

Item 17. Use this block to clarify any potential personnel security concerns (i.e., PR initiated and date, PR not initiated due to retirement within 12 months). Interim Access granted pending completed local files checks.

Item 18. This block must be signed by person authorized to validate the security clearance. Security manager/S2 cannot validate his/her own security clearance.

Bottom part of the FK Form 1378 should be used to document citizenship verification.

Always update the FK Form 1378 when a new security clearance is granted by CCF.

BLACK, Rose Ann		SGT	123-45-6789	3 Dec 07
1 NAME (Last, First, & Middle)		2 GRADE/RANK	3 SSN	4 DATE
5 DATE OF BIRTH 7 Jul 66	6 PLACE OF BIRTH Utica, NY		7 CITIZENSHIP (see reverse side) US	
8 ORGANIZATION A 3/16th	9 DUTY ASSIGNMENT, CIVILIAN POSITION TITLE & JOB NO S3, 3/16th CAV		10 CIVILIAN POSITION SENSITIVITY & CATEGORY/DATE APPROVED BY DSEC N/A	
11 DEGREE OF SECURITY CLEARANCE/ DATE GRANTED SECRET/15 Mar 06		12 DEGREE OF LOCAL ACCESS GRANTED Secret	13 DATE OF INITIAL SECURITY BRIEFING/ COMPLETION OF SF 312 3 Dec 07	
14 TYPE & DATE OF INVESTIGATION NACLC/1 Jan 06		15 SPECIAL ACCESS/DATE GRANTED (i.e., NATO, CNWDI, AR 50-5, etc.) CNWDI/3 Dec 07		
16 RECORDS CHECK CONDUCTED AND DATE			17 REMARKS	
PERSONNEL RECORDS 15 Nov 07				
UNIT FILES 1 Dec 07				
FINANCE RECORDS (Optional) N/A				
PMO RECORDS 20 Nov 07				
MEDICAL RECORDS 22 Nov 07				
INTELLIGENCE RECORDS 15 Nov 07				
18. NAME AND TITLE OF SECURITY MANAGER/S2 Mary Bell, Security Manager				
(Signature)				

FK FORM 1378-E, MAY 90

PREVIOUS EDITIONS MAY BE USED

RECORD OF PERSONNEL SECURITY CLEARANCE/ACTION
Intelligence Newsletter 87-1, 20 Feb 87

V1.40

CITIZENSHIP VERIFICATION

Documentation in subject's personnel file revealed the following information pertaining to citizenship status

Document NY Birth Certificate

U.S. citizen by birth in the U.S. U.S. citizen, but NOT born in U.S. NOT a U.S. citizen

PROOF OF CITIZENSHIP

*NAME (LAST, First, Middle) Jones, Rose Ann

*DOB (YMD) 7 Jul 66 *POB (State, County, City) Utica, NY

1 Birth Certificate Certificate Number 15934 M/D/Y Issued 01/15/70
Department of Issuance State Department County, City, State Utica, NY

2 Citizenship Certificate Certificate Number _____ M/D/Y Issued: _____
Department of Issuance _____ County, City, State _____

3 Naturalization Certificate Certificate Number _____ M/D/Y Issued: _____
Court _____ County, City, State _____

4 State Department Form 240 - Report of Birth Abroad of a Citizen of the U.S. M/D/Y Prepared _____

5 U.S. Passport (Current or Previous) Passport Number _____ M/D/Y Issued _____

6 DD FM 1966-5 - Item 41c Edition Date _____ (Must be Aug 85 or later edition)

Dual Citizenship Is (or was) subject a dual citizen of the U.S. and another country _____ (NO) _____ (YES)
(Country) (Dual citizenship must be reported to CCF along with an explanation from subject as to why dual citizenship is maintained)

Alien Place entered U.S. (City, State) _____ Date Entered _____
Alien Registration Number _____ Country of Citizenship _____

*As reflected on document used for citizenship verification

Date _____ Signature of Certifying Official (Name/Rank) _____

FK FORM 1378-E, MAY 90 (Back)

Appendix O
Security Access Roster

NUMBER	NAME	RANK	SSN	INVEST/DATE	CLN/DATE	ACTIVITY
1	SMITH JOE	GS07	123-45-6789	2-Apr-04	28-Apr-04	SEC DIV
2	SMITH JANE	GS08	234-56-7890	9-Jun-97	17-Jul-97	SEC DIV

(This page intentionally left blank)

Appendix P

Nomination for Access to Sensitive Compartmented Information (SCI)

LETTERHEAD IF NEEDED

IMSE-KNX-PLSO

Date

MEMORANDUM FOR Security Division, DPTMS (IMSE-KNX-PLSP)

SUBJECT: Nomination for Access to Sensitive Compartmented Information (SCI)

1. The below named individual is nominated for access to SCI:
 - a. Permanent access required:
 - b. Name:
 - c. SSN:
 - d. Aliases/Nickname:
 - e. Date and Place of Birth:
 - f. Rank:
 - g. Civilian/Military Status:
 - h. Reason for Request:
 - i. MOS:
 - j. Unit of Assignment:
 - k. U.S. Citizenship verified by:
 - l. Active Federal Service date without a break exceeding 24 months:

FOR OFFICIAL USE ONLY

IMSE-KNX-PLSO

SUBJECT: Nomination for Access to Sensitive Compartmented Information (SCI)

- m. Results of Local Records check/Date completed:
 - n. Adverse or Derogatory Information noted:
 - o. Spouse Full Name:
 - p. Spouse Place of Birth:
 - q. Spouse Citizenship:
 - r. SSBI Date:
 - s. Duty Position:
2. Point of Contact for this action is the undersigned at 4-XXXX.

JOHN DOE
COL, AR
Commanding

Appendix Q

Examples of Reportable Information (AR 380-67, appendix I)

INCIDENTS, INFRACTIONS, OFFENSES, CHARGES, CITATIONS, ARRESTS, SUSPICION, OR ALLEGATIONS OF:

- a. Disloyalty to the United States.
- b. Acceptance and maintenance of dual citizenship.
- c. Criminal or dishonest conduct (i.e., shoplifting, malingering, child abuse, use of force, violence, use of weapons).
- d. Mental or emotional problems or instability.
- e. Financial problems or unexplained affluence (i.e., bad checks, letters of indebtedness, bankruptcy, evidence of living beyond the individual's means).
- f. Drug/alcohol related incidents/abuse (i.e., self or command referral to drug/alcohol program, DUI/DWI, positive urinalysis, separation UP AR 635-200, chapter 9). **When the information is obtained through urinalysis testing, the information is NOT, repeat, NOT considered to be credible until a review of the positive results has been conducted by a physician assigned to perform medical review officer (MRO) functions IAW AR 600-85. Only after receipt of the MRO's findings and coordination with the local Staff Judge Advocate/Legal Advisor may the results be reported to CCF and the individual's access suspended.**
- g. Falsification.
- h. Refusal to answer significant security questions and/or refusal to submit required periodic reinvestigation.
- i. Refusal to execute a Nondisclosure Agreement, SF 312.
- j. Sexual misconduct (i.e., indecent exposure, rape, indecent acts with a minor, window peeping, and adultery).
- k. Foreign connections/vulnerability to blackmail.
- l. Acts that indicate poor judgment, irresponsibility, or untrustworthiness (i.e., AWOL/DRF, Article 15, court martial, driving while privileges are suspended, separation from U.S. Army UP Chapters 5, 7, 10, 11, 13, 14, & 15, AR 635-200).

(This page intentionally left blank)

(This page intentionally left blank)

**Appendix S
Suspension of Access to Classified Information**

Sample Memorandum for Suspension of Access to Classified Information

LETTERHEAD IF NEEDED

OFFICE SYMBOL

Date

MEMORANDUM FOR LAST NAME, First Name, Middle Initial, RANK, SSN, Unit of Assignment

SUBJECT: Suspension of Access to Classified Information

1. Reference AR 3800-57, paragraph 8-102, Department of the Army Personnel Security Program Regulation.
2. You are hereby notified that your access to classified defense information has been suspended pending adjudication and a final security determination by the Commander, U.S. Central Personnel Security Clearance Facility (CCF). This action is based upon the following information which raises serious questions as to your ability or intent to protect classified information:

(Summarize all unfavorable information used as a basis for the suspension.)
3. You are directed to acknowledge receipt of this memorandum by signing and dating the enclosed response.
4. You will be notified as expeditiously as possible of CCF's final determination.
5. Point of contact.

Encl

SIGNATURE BLOCK
Cdr/S2/Security Manager

FOR OFFICAL USE ONLY

Sample Acknowledgment for Suspension of Access to Classified Information

OFFICE SYMBOL

Date

MEMORANDUM FOR S2/Security Manager, Unit Designation

SUBJECT: Receipt of Acknowledgement

1. I, (Print full name and SSN), acknowledge that I have been informed in writing that my access to classified defense information was suspended and the basis thereof.
2. I understand that I am not authorized any access to classified defense information unless notified by my commander or S2/security manager that a favorable determination was made by the Commander, CCF.

RANK/ Signature

Date

CF:
Security Division, DPTMS

FOR OFFICIAL USE ONLY

Appendix T Rebuttal Guidelines

Sample Statement of Rebuttal Guidelines

T-1. The following guidelines are provided for use in preparing your statement of rebuttal:

a. Explain, rebut, refute, or mitigate each incident or issue raised in CCF's letter of intent (LOI). Provide all relevant and extenuating circumstances surrounding the incident, to include conditions which directly or significantly contributed to your conduct (such as divorce action, death in family, severe provocation, immaturity due to your age at the time of the incident).

b. Be specific, provide substantiating documentation, if available (i.e., receipts, medical reports, court files, character testimonies, etc.) and write your statement so as to portray your conduct in a more favorable light. Appendix I to AR 380-67 indicates various circumstances which may mitigate disqualifying information. It would be to your advantage to familiarize yourself with the mitigating factors and mention all factors in your statement of rebuttal which apply.

c. Provide information that would attest to your loyalty, reliability, and trustworthiness. Back this up with letters of recommendations from employers, supervisors, friends, etc. Letters of recommendations should indicate how long the individual has known you, what type of person you are, and whether they feel you are trustworthy and responsible enough to be entrusted with classified information.

d. Describe all actions you have taken to change your conduct or behavior. Include a personal assurance that you will not involve yourself in the future in any action that could cast doubt on your loyalty, reliability, or trustworthiness.

T-2. This proposed action should not be treated lightly. An unfavorable determination could have very serious repercussions. You may seek legal assistance; however, any cost incurred would be at your own expense. Military personnel may seek advice from Legal Assistance Office, Staff Judge Advocate (624-2771).

T-3. You have 50 days from the date of acknowledgment to submit your rebuttal to the G2/Intelligence. This will allow 10 extra days to ensure the action is received by CCF within the 60 days suspense period they assigned. If you decide not to submit a statement of rebuttal, please notify your unit security manager immediately.

T-4. Your statement of rebuttal must be signed by you and endorsed by your chain of command. Your commander must recommend whether your security clearance should be denied, revoked, or restored and provide his/her rationale, addressing the issues outlined in the LOI. Any response that does not include your commander's recommendation will be returned. If you have engaged an attorney for legal advice and assistance, it is still your responsibility for preparation, signing, and submitting your statement to your company commander. Your statement should be

Fort Knox Pam 380-67 (24 Jul 08)

turned in to your company commander for comments within approximately 43 days of receipt of acknowledgment. It is to your advantage to keep a copy of all correspondence you have prepared and received pertaining to your LOI.

T-5. If you require an extension of the suspense date, contact your unit security manager. Be prepared to provide justification for the extension and an expected completion date.

T-6. If you need any assistance feel free to contact _____, your unit security manager, 624-_____, or any representative of the Security Division, DPTMS, 4-6741/2814.

Sample Subject's Memo to CCF

LETTERHEAD

OFFICE SYMBOL

Date

MEMORANDUM THRU Chief, Security Division, DPTMS (IMSE-KNX-PLSP), 201 6th Ave, Suite 48, U.S. Army Garrison Command, Fort Knox, KY 40121-5721

FOR Commander, U.S. Army Central Personnel Security Clearance Facility (PCCF), 4552 Pike Road, Fort George G. Meade, MD 20755-5250

SUBJECT: Statement of Rebuttal (Indicate your Last Name, First Name, Middle Initial, Rank, Social Security Number, Unit of Assignment)

1. Reference memorandum, CCF, PCCF (date of Letter of Intent), subject: (type as appears in memorandum).
2. Start your memorandum by addressing each issue raised in CCF's LOI.
 - a.
 - b.
3. Finalize your action by explaining your rationale as to why you should be allowed to retain or be granted a security clearance.

Encl

YOUR SIGNATURE

FOR OFFICIAL USE ONLY

(This page intentionally left blank)

Appendix U

Initial Security Briefing

1. Safeguarding defense information is everyone's responsibility. Security is defined as the proper and effective safeguarding of a command and its personnel against any conceivable enemy action; however, this briefing is concerned primarily with the security of classified information.

2. Classification of Information. Military information is classified, when necessary, to protect it from unnecessary disclosure to unauthorized persons or agencies. Unauthorized persons or agencies include any person, group, or agency that is not properly cleared or does not have a need to know the information in question. Degrees of classification are as follows:

a. **TOP SECRET.** Defense information classified TOP SECRET is information where disclosure to an unauthorized person could result in exceptionally grave danger to the defense of the United States.

b. **SECRET.** Defense information classified SECRET is information where disclosure to an unauthorized person could result in serious damage to the defense of the United States.

c. **CONFIDENTIAL.** Defense information classified CONFIDENTIAL is information where disclosure to an unauthorized person could be detrimental to the defense of the United States.

3. Personnel Security Clearances.

a. Authorization to obtain classified information is called access. A security clearance only represents initial authority to access classified information. Access to classified information is granted only after the need-to-know basis has been established.

b. A security clearance is granted to individuals only after an examination of their background and record show they are responsible, reliable, of good character, and can be trusted not to divulge sensitive or classified information to unauthorized personnel.

c. Levels of access to classified information must correspond to no higher than the degree of clearance granted.

d. A security clearance will be validated only when there is an official requirement for the clearance. Individuals may not request a security clearance for themselves because they want one or solely because of their rank.

e. Security clearances must be validated at each new duty station before access to classified information is granted. Security clearances are only validated after local background checks through the post MILPO and medical records facilities are conducted.

f. An individual's trustworthiness to hold a security clearance is a continuing assessment.

The responsibility for such assessment is shared by your chain of command, security manager, and supervisor. As such, you are continually observed with respect to security clearance eligibility. You must be aware of the standards of conduct required for persons holding positions of trust. You must also recognize and avoid the kind of personal behavior that could result in rendering you *ineligible to keep your security clearance or continued assignment in a position of trust* (i.e., excessive indebtedness; criminal or dishonest conduct; deliberate false statement; habitual or abusive use of intoxicating beverages, narcotics, drugs or controlled substances; disregard of public law; emotional instability; etc.). In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with YOU.

4. Correct Handling and Protection.

a. Documents containing classified information are marked at the top and bottom of each page with the appropriate classification level. Documents with no classification markings do not normally require special protection.

b. When a classified document is removed from storage, it should be protected with a cover sheet. Cover sheets are brightly colored (blue for CONFIDENTIAL, red for SECRET, and orange for TOP SECRET) and prominently labeled to identify the documents as classified. A cover sheet also protects any classified information appearing on the front page of a document from being read by unauthorized personnel. Do not leave classification cover sheets lying around; they should be placed in file folders (by classification markings) and locked in a file container.

c. Classified documents must be attended (*guarded*) or secured (*locked up in authorized GSA safes*). Leaving a classified document unsecured and unattended is a serious breach of security, which could lead to compromise of the classified information contained therein.

d. Classified waste material, such as handwritten notes, carbon paper, typewriter ribbons, and working papers that contain classified information must be protected to prevent unauthorized disclosure. Each will be marked accordingly to the highest degree of classified information contained and must be secured in an approved container when not under control of an authorized individual.

e. Copying classified information on copiers is strictly prohibited at your level.

f. Transmission. Classified documents can be hand carried or escorted from one location to another by a properly cleared and qualified individual. You must have, in your possession, a valid DD Form 2501 (courier card) or a memorandum from the security manager granting approval to hand carry classified material. CONFIDENTIAL documents may also be transmitted by certified mail and SECRET documents by registered mail. Classified material which is sent by mail is doubled wrapped with only the inner wrapping depicting the classification of the contents; the outer wrapping shows no classification. Hence, any unopened item of certified mail may contain CONFIDENTIAL material, and any unopened items of certified or registered mail must be protected as classified material.

g. Individuals having knowledge of classified information, whether received through contact with classified material, presentations, briefings, or through any other means, have an obligation to protect this information from unauthorized disclosure. Studies have shown that more classified defense information is compromised because of loose talk and carelessness during social conversation than in any other way. This type of compromise is doubly dangerous, because it often goes unrecognized and unreported. Only discuss classified information with individuals who are properly cleared and have a valid NEED TO KNOW and only in a proper setting. Report any security violations to your security manager. If you ever see a classified document lying in a place where it can be read by unauthorized persons, immediately protect it and turn it in to your security manager or chain of command.

h. Destruction. Classified documents which have outlived their usefulness must be destroyed in such a way the remains cannot be reconstructed to indicate the original contents. Destruction is usually accomplished by shredding and burning (including total crumbling of the ashes). Destruction of classified material will be accomplished by the security manager only.

5. Questions concerning this briefing should be directed to your security manager.

Printed Name & Date

S-2/Security Manager Name & Date

Signature

Signature

(This page intentionally left blank)

Appendix V
DA Form 2962, Security Termination Statement

SECURITY TERMINATION STATEMENT For use of this form, see AR 380-5; proponent agency is OACSI. <small>For use of this form, see AR 380-5, the proponent agency is OACSI.</small>		DATE		
PART I - BASIC INFORMATION				
FROM (Originating Headquarters)				
NAME (Last, first, middle initial)	GRADE (Mil or Civ)	SOCIAL SECURITY NUMBER		
PART II - REFERENCES				
<p>A. APPLICABLE TO ALL PERSONNEL WHO HAVE HAD ACCESS TO DEFENSE INFORMATION (1) ESPIONAGE LAWS: TITLE 18, U.S. CODE, SECTIONS 793, 794, AND 798. (<i>Temporary extension of Section 794</i>) (2) INTERNAL SECURITY LAWS: TITLE 50, U.S. CODE, SECTION 783. (3) DOD REGULATION 5200.1-R, AR 380-5.</p> <p>B. ADDITIONALLY APPLICABLE TO PERSONNEL WHO HAVE HAD ACCESS TO RESTRICTED DATA (1) ATOMIC ENERGY ACT OF 1954: TITLE 42, U.S. CODE, SECTIONS 2014, 2162, 2274, 2275, 2276, AND 2277. (2) AR 380-150.</p> <p>C. OTHER (Specify)</p>				
PART III - SECURITY TERMINATION AND DEBRIEFING STATEMENT				
<p>1. I acknowledge that I have read the applicable material for the level of classified information to which I have had access, and I understand that the revelation of classified information to an unauthorized person or agency is prohibited and punishable by law. My initials below attest to the level of access which I have had and to the applicable material, as identified in References, which I have read.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 40%; vertical-align: top;"> INITIALS _____ _____ _____ </td> <td style="width: 60%; vertical-align: top;"> EXTENT OF ACCESS a. TOP SECRET - SECRET - CONFIDENTIAL defense information (Reference a). b. RESTRICTED DATA (Reference b). c. Other (Specify) </td> </tr> </table>			INITIALS _____ _____ _____	EXTENT OF ACCESS a. TOP SECRET - SECRET - CONFIDENTIAL defense information (Reference a). b. RESTRICTED DATA (Reference b). c. Other (Specify)
INITIALS _____ _____ _____	EXTENT OF ACCESS a. TOP SECRET - SECRET - CONFIDENTIAL defense information (Reference a). b. RESTRICTED DATA (Reference b). c. Other (Specify)			
<p>2. I do not have classified material or documents in my possession.</p> <p>3. I will not divulge classified information orally, in writing, or by any other means, to an unauthorized person or agency.</p> <p>4. I will immediately report to the Federal Bureau of Investigation, my superior commander, or other military authority, as appropriate, any attempt by an unauthorized person or agency to obtain classified information.</p> <p>5. I received an oral debriefing, immediately prior to the execution (i.e., signature) of this Security Termination Statement.</p>				
DISTRIBUTION FIELD 201 FILE (Military) LOCAL SECURITY FILE	SIGNATURE			

OUTLINE OF GENERAL CONTENT ORAL SECURITY DEBRIEFING

(Part of Security Termination Statement)

1. PURPOSE OF DEBRIEFING. a. To establish that the individual does in fact understand the implications, to national security, and to him/her self, of the statutes and regulations which he/she has read.
b. To emphasize to the individual that he/she was afforded access to classified information solely because of his/her "need-to-know" in the performance of official duties; that this information was entrusted, as well as officially charged to him/her; and that his/her impending separation, in no way lessens his/her responsibilities - and liabilities - for ensuring that the classified knowledge acquired is not divulged in any manner to an unauthorized person or agency.
2. SERIOUS NATURE OF THE SUBJECT MATTER WHICH REQUIRES PROTECTION. Emphasize to the individual that classified information is defined and described in the pertinent statutes and regulations which he/she has read. As an illustration, cite the fact that *SECRET* defense information is "information or material the unauthorized disclosure of which *COULD RESULT IN SERIOUS DAMAGE TO THE NATION*". Where the individual has had access to *TOP SECRET, RESTRICTED DATA*, compartmented information, cite the specific definition(s) and description(s) and emphasize that such material is even more serious in nature.
3. NEED FOR CAUTION AND DISCRETION. a. Emphasize to the individual that the responsibility is *HIS/HER'S* to specifically establish that a person or agency requesting any classified information is officially authorized (*NEED-TO-KNOW*) that information; that if he/she is leaving the service (*includes civilian employees*), absolutely no other person or agency is authorized the classified information.
b. Emphasize to the individual that the mere fact that he/she reads a news article which appears to contain classified information in no way authorizes him/her to confirm or deny the item. Explain that good "guesses" frequently are reflected by the news media, but bad "guesses" and incorrect information also are included.
c. Caution the individual that history records a number of cases involving unauthorized disclosures in clubs and at social gatherings which have been reported and which resulted in punitive action.
4. SUMMARY. Specifically ask the individual if he understands what he/she has read and what he/she is about to sign. Based on his/her response (*and questions he/she may raise*) re-emphasize the content of the Security Termination Statement.