BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-501

1 AUGUST 2000

8TH FIGHTER WING COMMAND
Supplement 1

13 FEBRUARY 2004

Security

PERSONNEL SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ USAF/XOFI
(Ms. Jean Smith/Linda Patten)
Supersedes AFI 31-501, 2 May l994 and AFH 31-502, 1 May 1996

Certified by: HQ USAF/XOF
(Brig Gen James M. Shamess)
Pages: 91
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 31-5, *Personnel Security Program Policy*. It provides guidance for personnel security investigations and clearance needs. **Use this instruction with** Department of Defense (DOD) Regulation 5200.2-R, *DOD Personnel Security Program*, January 1987, and Executive Order 12968 "Access to Classified Information."

(8FW) This supplement implements AFI 31-501, *Personnel Security Program Management.* Commanders and Staff Agency Chiefs are responsible for the protection of property under their jurisdiction, administration, custody, and control. Specifically, they will ensure requirements and procedures established in AFI 31-501/8 FW Supplement 1, are met. It applies to all units assigned, attached, or associated units to the 8th Fighter Wing, Kunsan Air Base, Korea.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This instruction aligns with DOD 5200.2-R and AFPD 31-5. It **updates and clarifies:** time frames to submit personnel security questionnaires; when waivers of pre-employment investigative requirements may be used; procedures for limited access authorizations (LAA); conditions when access to classified information at a higher level may be granted; investigative requirements for the Nuclear Weapon Personnel Reliability Program (PRP); investigative process for individual mobilization augmentees and individual ready reservists; the fact that only criminal investigations may be requested from AFOSI; procedures for "For Cause" discharge of individuals with SCI access; that the 497 IG/INS (Central Adjudication Facility (CAF)) is the authority to (1) close established Security Information Files (SIF); and (2) request a Special Investigative Inquiry from the Defense Security Service (DSS); **adds guidance for:** access by

different categories of personnel; Presidential Support Program (PSP) procedures; Security Information File (SIF) procedures; due process procedures; civilians occupying nonsensitive positions procedures; nonappropriated fund employees suitability procedures; submitting periodic reinvestigations; mandatory investigation requirements for AF specialty codes; permanent membership on the Personnel Security Appeal Board; SENTINEL KEY (SK) as the replacement for the Automated Security Clearance Approval System (ASCAS); actions to be taken concerning an individual's suitability when the security clearance is in question; periodic reinvestigations on personnel assigned to a NATO staff position; foreign nationals needing unescorted entry to restricted areas; processing the Electronic Personnel Security Questionnaire (EPSQ); results of investigations for access to unclassified Automated Information Systems (AIS) (formerly Automated Data Processing, (ADP)) being returned to authorized requesters for commander's suitability determination; implementation of new Single Scope Background Investigation (SSBI), periodic reinvestigation (PR) scope, and National Agency Check with Local Agency Checks and Credit Check (NACLC) for military accessions (instead of the Entrance National Agency Check) and secret security eligibility (instead of the National Agency Check); obtaining access to the Defense Clearance and Investigation Index (DCII); **includes:** sample figures for processing PSP requirements; sample figures for processing SIF requirements; sample figure for pre-employment waiver; sample figure and instructions for processing AF Form 2583, **Request for Personnel Security Action**; definition for DCID 6/4 (formerly DCID 1/14); **deletes the requirement:** to file a copy of the personnel security questionnaire in military and civilian official personnel files; for the servicing security activity to make a recommendation to commanders on granting of unescorted entry to restricted areas; for SCI and special access program foreign travel restrictions; for AFOSI personnel to refer foreign travel to local AFOSI commander; for supervisors to review individual's completed personnel security questionnaires for a periodic reinvestigation when conducting the supervisory certification; to send unit manning document changes through the security forces; for the CAF to grant security clearance authority for civilians occupying nonsensitive positions; for routine prescreening interviews for SCI access; for billets management of TS positions; **authorizes:** individuals 60 days to rebut a letter of intent to deny or revoke a security clearance; commanders to grant interim Top Secret and Secret security clearances for civilian and military members; commanders options for granting unescorted entry for contractors acting as visitor groups (long term contractors); commanders to waive investigative requirements, on a case by case basis, for unescorted entry to restricted areas and access to unclassified AIS; MAJCOM commanders to waive investigative requirements for mobilization of DOD civilian retirees with a break in service of more than 24 months; active Senior Executive Service (SES) member to grant access to retired flag or general officer or SES member; temporary access for NATO COSMIC Top Secret based on final US Secret clearance; the CAF as approval authority for DCII; **changes:** the office of primary responsibility from HQ USAF/XOFI to the CAF for the LAA program; the period when access to classified information may be granted to retired general officers from 90 days to 180 days; the time limit from 24 to 12 months before requests for reinstatement of security clearances are authorized; the requirement for Secret periodic reinvestigations from 15 years to 10 years; the Catch'Em in CONUS questionnaire completion date from 90 days to 180 days; and **requires:** authorized requesters to consult the DCII and the Clearance and Access Verification System (CAVS) on the status of investigations prior to commanders granting interim security clearances; commanders to: (1) validate positions requiring access to classified information annually and (2) personally ensure implementation of the personnel security program at every level of command.

(8FW) This supplement supersedes 8 FW Sup 1 of AFI 31-501 dated 2 November 2001. It reflects the requirements instituted by AFI 31-501. The latest version of the Electronic Personnel Security Questionnaire (EPSQ) will be used when submitting requests for personnel security investigations (paragraph **5.1.1.2. (Added)**). SMs will complete each individual's AF Form 2583, *Request for Personnel Security*

Action. AF Form 2583s submitted to 8 SFS/SFAIP must be re-accomplished if the signatures by the SM and 8th Medical Operations Squadron, Flight Medicine (8 MDOS/SGOAF) personnel exceed 30 days (paragraph **5.4.1. (Added)**). Personnel, who are not Security Access Requirement (SAR) coded at Kunsan AB and require a periodic reinvestigation or clearance upgrade for an upcoming assignment, must obtain a security requirement letter from 8 MSS/DPMAR stating the type clearance required. This letter must be brought to 8 SFS/SFAIP along with the other clearance material prior to submission to the investigating agency (paragraph **5.4.2. (Added)**). Personnel Security Investigations (PSI) will be submitted within 30 days of notification from the unit SM. SMs are responsible for tracking the date the individual was notified. ***NOTE:*** Failure to provide the PSI within the above timeframe is grounds for Security Information File (SIF) establishment (paragraph **5.6.1.1. (Added)**). A bar (|) indicates revisions from the previous edition.

(8FW) AFI 31-501, dated 1 August 2000 is supplemented as follows:

Chapter 1—GENERAL PROVISIONS **8**

1.1. Purpose. 8

1.2. Applicability. 8

1.3. Definitions. 8

1.4. Records Management. 8

Chapter 2—POLICIES **9**

2.1. Clearance and Sensitive Position Standard. 9

2.2. Military Service Standard. 9

2.3. Criteria for Application of Security Standards 9

2.4. Types and Scope of Personnel Security Investigations. 9

2.5. Authorized Personnel Security Investigative Agencies. 10

2.6. Allegations of Criminal Activity. 10

2.7. Overseas Personnel Security Investigations. 10

2.8. Limitations and Restrictions. 10

Chapter 3—SECURITY CLEARANCE **11**

3.1. Authority to Designate Sensitive Positions. 11

3.2. Nonsensitive Positions. 11

3.3. Reassignment to a Noncritical Sensitive Position. 11

3.4. Reassignment to a Critical Sensitive Position. 11

3.5. PRs for Critical Sensitive and Noncritical Sensitive Positions. 12

3.6. Pre-employment Waivers. 12

3.7. Mobilization of DOD Civilian Retirees. 12

3.8. Military Appointment, Enlistment, and Induction. 12
3.9. Mobilization of Military Retirees. 12
3.10. Security Clearance Authority. 12
3.11. Interim Security Clearances. 13
3.12. Access to Classified Information by Non-US Citizens. 13
3.13. Access by Persons Outside the Executive Branch. 14
3.14. Access by Different Categories of Individuals. 14
3.15. One Time Access. 15
3.16. Processing Requests for Access by Retired General Officers or Civilian 15
3.17. Processing Requests for Access by Historical Researchers. 15
3.18. Sensitive Compartmented Information. 16
3.19. Single Integrated Operational Plan-Extremely Sensitive Information. 16
3.20. Presidential Support Activities. 16
3.21. Nuclear Weapons Personnel Reliability Program. 18
3.22. Access to North Atlantic Treaty Organization Classified Information. 19
3.23. Special Access Program. 19
3.24. Processing Requests for Access to Restricted Areas, Sensitive Information 19
3.25. Nonappropriated Fund Employees. 20
3.26. Special Agents and Investigative Support Personnel. 20
3.27. Personnel Occupying Information Systems Positions Designated Auto 20
3.28. Periodic Reinvestigations. 21

Chapter 4—RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS 22

4.1. Prior Federal Civilian Investigations. 22

Chapter 5—REQUESTING PERSONNEL SECURITY INVESTIGATIONS 23

5.1. General. 23
5.2. Authorized Requesters. 23
5.3. Criteria for Requesting Investigations. 23
5.4. Request Procedures. 23
5.5. Priority Requests. 24
5.6. Personal Data Provided by the Subject of the Investigation. 24

Chapter 6—ADJUDICATION **25**
6.1. Central Adjudication Authority. 25
6.2. Adjudicative Record. 25

Chapter 7—ISSUING CLEARANCE AND GRANTING ACCESS **26**
7.1. General. 26
7.2. Investigative Requirements for Air Force Specialty Codes. 26
7.3. Issuing Security Clearance. 26
7.4. SENTINEL KEY. 26
7.5. Granting Access. 29
7.5. (8FW)Granting Access. 29
7.6. Obtaining Information from the CAF. 29

Chapter 8—UNFAVORABLE ADMINISTRATIVE ACTIONS **30**
8.1. Referral for Action. 30
8.2. Suspension. 30
8.3. Air Force Office of Special Investigations. 35
8.4. Final Unfavorable Administrative Actions. 35
8.5. Procedures. 35
8.6. Unfavorable Administrative Action Procedures. 35
8.7. Security Clearance Reinstatement. 37
8.8. Special Access Programs. 37
8.9. Obtaining Permission to Proceed in Courts-Martial, Administrative Dis 37

Chapter 9—CONTINUING SECURITY RESPONSIBILITIES **40**
9.1. Evaluating Continued Security Clearance. 40
9.2. Supervisory Responsibility. 40
9.3. Initial Briefings and Refresher Briefings. 40
9.4. Foreign Travel Briefing. 40
9.5. Termination Briefing. 40

Chapter 10—SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS **41**
10.1. Responsibilities. 41
10.2. Access Restrictions. 41
10.3. Safeguarding Procedures. 41

Chapter 11—PROGRAM MANAGEMENT **42**

11.1. Responsibilities. 42

Chapter 12—DEFENSE CLEARANCE AND INVESTIGATIONS INDEX **43**

12.1. Access. 43

12.2. Investigative Data. 43

12.3. Disclosure of Information. 43

12.4. Forms Prescribed. 43

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION **44**

Attachment 1 (8FW)—GLOSSARY OF REFERENCES, ABBREVIATIONS AND ACRONYMS **51**

Attachment 2—REQUEST PROCEDURES **52**

Attachment 3—TABLES FOR INVESTIGATIONS AND ASSIGNING SECURITY ACCESS REQUIREMENTS (SAR) **57**

Attachment 4—DOD SECURITY CLEARANCE AND OR SCI ACCESS DETERMINATION AUTHORITIES **64**

Attachment 5—STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD **66**

Attachment 6—SAMPLE WAIVER OF PRE-APPOINTMENT INVESTIGATIVE REQUIREMENTS **68**

Attachment 7—SAMPLE MEDICAL CERTIFICATION TO THE COMMANDER OF INDIVIDUAL FOR PRESIDENTIAL SUPPORT PROGRAM **69**

Attachment 8—SAMPLE COMMANDER'S NOMINATION TO CHIEF, SERVICING SECURITY ACTIVITY FOR A PRESIDENTIAL SUPPORT POSITION **70**

Attachment 9—SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, MEMORANDUM TO 497 IG/INS FOR PROCESSING OF PRESIDENTIAL SUPPORT PROGRAM NOMINEE **72**

Attachment 10—SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, NOTIFICATION TO THE SERVICING MEDICAL FACILITY OF THE INDIVIDUAL APPROVED FOR PRESIDENTIAL SUPPORT DUTIES **73**

Attachment 11—SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, REQUEST FOR EVALUATION OF CONTINUED SECURITY CLEARANCE TO COMMANDER 74

Attachment 12—SAMPLE REQUEST TO ESTABLISH A SECURITY INFORMATION FILE (SIF) 76

Attachment 13—SAMPLE COMMANDER NOTIFICATION TO INDIVIDUAL OF SIF ESTABLISHMENT AND SUSPENSION OF ACCESS TO CLASSIFIED INFORMATION 78

Attachment 14—SAMPLE COMMANDER NOTIFICATION TO INDIVIDUAL OF SIF ESTABLISHMENT WITH CONTINUED ACCESS TO CLASSIFIED INFORMATION 80

Attachment 15—SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, NOTIFICATION TO COMMANDER OF SIF ESTABLISHMENT 81

Attachment 16—SAMPLE SIF CUSTODIAN CHECKLIST ITEMS 83

Attachment 17—SAMPLE NOTIFICATION TO 497 IG/INS OF SIF ESTABLISHMENT WHEN INDIVIDUAL MAINTAINS ACCESS 84

Attachment 18—SAMPLE SIF ESTABLISHMENT NOTIFICATION TO INSTALLATION COMMANDER 85

Attachment 19—SAMPLE REQUEST FOR REVIEW AND WRITTEN OPINION 86

Attachment 20—SAMPLE SIF TRANSFER MEMORANDUM TO GAINING SECURITY ACTIVITY 87

Attachment 21—SAMPLE RECOMMENDATION TO 497 IG/INS FOR SIF CLOSURE 88

Attachment 22—INSTRUCTIONS FOR MAILING EPSQ DISKETTE TO DSS 89

Attachment 23—INSTRUCTIONS TO COMPLETE AF FORM 2583, REQUEST FOR PERSONNEL SECURITY ACTION 90

Chapter 1

GENERAL PROVISIONS

1.1. Purpose.

1.1.1. **Use this instruction with the DOD Regulation 5200.2-R and AFPD 31-5** to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968**;** and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013. Privacy Act system of records notices F031 497IG A, SCI Personnel Records; F031 497IG B Special Security Case Files; F031 11 SPS A, Presidential Support Files; F031 11 SPS B, Personnel Security Clearance and Investigation Records; F031 AF SP N, Special Security Files; .F031 SAFPA A, Requests for Access to Classified Information by Historical Researchers; F036 497 IG B, For Cause Discharge Program apply.

1.1.2. Submit waivers to DOD Regulation 5200.2-R and AFPD 31-5 through command Information Security Program Manager (ISPM) channels to HQ USAF/XOFI, 1340 Air Force Pentagon, Washington DC 20330-1340.

1.2. Applicability. This AFI applies to DOD civilian employees, active duty military, the Air National Guard and Air Force Reserves.

1.3. Definitions. See Atch 1 for additional definitions. For purposes of this AFI the term “Commander” includes “Staff Agency Chiefs.”

1.4. Records Management. Maintain and dispose of all records created as a result of prescribed processes in accordance with AFMAN 37-139 , Records Disposition Schedule.

Chapter 2

POLICIES

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

2.2. Military Service Standard. See AFPD 36-29, *Military Standards* and AFPD 36-20, *Accession of Air Force Military Personnel.* It provides policies to ensure the Air Force employs the right quantity and quality of people in the Air Force.

2.3. Criteria for Application of Security Standards . The criteria for determining eligibility for a security clearance are listed in DOD 5200.2-R, para 2-200. Commanders apply the criteria for security standards when granting access to classified information.

2.4. Types and Scope of Personnel Security Investigations. The scope of each type of personnel security investigation is listed in DOD 5200.2-R, Appendix B. See Atch 2 for procedures on requesting personnel security investigations (PSIs). See Atch 3 for tables on required investigations and the assignment of security access requirement (SAR) codes.

2.4.1. General. The investigations listed in DOD Regulation 5200.2-R and this instruction are the only PSIs authorized. The Secretary of the Air Force and or the Assistant Secretary of Defense for Command, Control, Communications and Intelligence must approve raising or lowering the scope of the authorized investigation type.

2.4.2. Entrance National Agency Check (ENTNAC). ENTNACS were replaced by the NACLC on 1 Oct 99 for military accessions.

2.4.3. National Agency Check (NAC). NACs are primarily used for positions of trust.

2.4.4. National Agency Check Plus Written Inquiries and Credit Check (NACIC). NACICs are conducted by OPM and are required on all civilian employees entering government employment and assigned to nonsensitive positions.

2.4.5. Access National Agency Check with Written Inquiries and Credit Check (ANACI). ANACIs are conducted by OPM and are required for civilian employees' initial Secret security clearance or assignment to noncritical sensitive positions.

2.4.6. National Agency Check, Local Agency Checks and Credit Check (NACLC). NACLCs are required for military access to Secret information.

2.4.7. Single Scope Background Investigation (SSBI). SSBIs are required for access to TOP SECRET, Sensitive Compartmented Information (SCI), special sensitive positions and for critical sensitive positions.

2.4.8. Periodic Reinvestigation (PR). PRs are investigations conducted at prescribed intervals for the purpose of updating a previously completed background investigation.

2.4.9. Special Investigative Inquiry (SII). SIIs are used to prove or disprove allegations or new information concerning the security standards that arise after a person has been granted a security clearance.

2.5. Authorized Personnel Security Investigative Agencies. The Defense Security Service (DSS) and the Office of Personnel Management (OPM) conduct Personnel Security Investigations for the Air Force.

2.6. Allegations of Criminal Activity. Commanders refer possible criminal conduct to the supporting Air Force Office of Special Investigations (AFOSI) detachment.

2.7. Overseas Personnel Security Investigations. AFOSI personnel conduct the DSS portion of PSIs in overseas areas augmented by their Army, Navy, and State Department counterparts.

2.8. Limitations and Restrictions. A break in service of over 24 months invalidates an individual's personnel security clearance eligibility.

Chapter 3

SECURITY CLEARANCE

3.1. Authority to Designate Sensitive Positions. Commanders with position designation authority determine the security sensitivity of civilian positions. Each civilian employee is subject to an investigation depending on the sensitivity of the position to be occupied, except for reappointment when the break in employment is less than 24 months.

3.2. Nonsensitive Positions.

3.2.1. The servicing civilian personnel flight (CPF) processes the initial request for NACIC's to OPM for civilians occupying nonsensitive positions, not requiring access to classified information. OPM forwards the investigation to the CAF. Suitability determinations for civilian government employment are made accordingly:

3.2.2. The CAF forwards the completed investigation, OPM "Certificate of Investigation" and the OPM INV Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations to the base servicing CPF.

3.2.3. The CPF:

3.2.3.1. Determines if the individual is deemed suitable for employment IAW 5 CFR 731.201-202. Coordination and or consultation with the supervisor and or commander may be made.

3.2.3.2. If employee is determined suitable, CPF signs off on the OPM Certificate of Investigation and the form is filed in the individual's Official Personnel Folder (OPF) IAW AFI 36.114, *Guide to Personnel Recordkeeping*.

3.2.3.3. If applicant is determined unsuitable, CPF fills out the OPM INV Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations and coordinates with the employee's supervisor and or commander. CPF forwards the OPM INV Form 79A to OPM.

3.3. Reassignment to a Noncritical Sensitive Position. If a civilian employee is subsequently selected for a position requiring access to classified information and unescorted entry into restricted areas (noncritical sensitive), security managers process the completed SF 86, **Questionnaire for National Security Positions**, to security forces authorized requesters.

3.3.1. Security Forces Authorized Requesters:

3.3.1.1. Submit the SF 86 to OPM for an "Access NACI". The address is: OPM-FIPC PO Box 618, 1137 Branchton Road, Boyers, PA, 16018. OPM does not have the EPSQ, therefore requests must be sent in hard copy. Use the EPSQ at the unit, validate the EPSQ, and print the SF 86 for mailing. Contact the servicing CPF for any questions concerning Part 1 of the SF 86 or the OPM Agency Use Information Sheet. A fingerprint card is not required as the individual has already been the subject of a NACI or NACIC.

3.4. Reassignment to a Critical Sensitive Position. If, in the future, the individual is selected for a critical sensitive position, security managers process the request for investigation to the security forces authorized requester who will submit an SF 86 requesting a SSBI in accordance with Atch 2.

3.5. PRs for Critical Sensitive and Noncritical Sensitive Positions. The periodic reinvestigation requirements apply to civilian employees in noncritical sensitive positions that require access to classified information. The reinvestigation requirements apply to civilian employees in critical sensitive positions whether or not they have access to classified information. See Atch 3.

3.6. Pre-employment Waivers.

3.6.1. Sensitive Positions. Commanders must ensure procedures for pre-appointment to sensitive positions preclude an uncleared person from having access to classified information.

3.6.2. Noncritical Sensitive and Critical Sensitive Positions (3-204). The commander or staff agency chief (or designee) with position sensitivity determination authority prepares a waiver of pre-employment investigation requirements when such action is necessary and in the national interest. See Atch 6 for sample waiver memorandum. The memorandum is filed in the individual's OPF IAW AFI 36-114, *Guide to Personnel Recordkeeping*.

3.7. Mobilization of DOD Civilian Retirees. MAJCOM commanders can waive the investigative requirements for the mobilization of selected re-employed annuitants for temporary appointment when the break in employment is greater than 24 months.

3.8. Military Appointment, Enlistment, and Induction. Personnel appointed, enlisted, or inducted to the active or reserve forces of the Air Force must have a favorable personnel security investigation. See Atch 3.

3.8.1. Clearance requirements for officer training school selectees are outlined in Air Force Instruction (AFI) 36-2005, *Appointment in Commissioned Grades and Designation and Assignment in Professional Categories*.

3.9. Mobilization of Military Retirees. MAJCOM commanders can waive the requirement for a full NACLC for the mobilization of military retirees upon reentry to active duty after a break of more than 24 months.

3.10. Security Clearance Authority. The 497 Intelligence Group/INS, Directorate of Security and Communications Management, the Air Force Central Adjudication Facility, is the designated authority to grant, suspend, deny, or revoke personnel security clearances and SCI access (see Chapter 11).

3.10.1. The CAF issues security clearance eligibility to the highest level authorized based on the type of investigation conducted. Unit commanders grant clearance access based on the level of the position occupied by the individual. The access level required should be annotated on the request for investigation.

3.10.2. The SAF Special Access Program (SAP) Central Adjudication Office, Wright-Patterson AFB Ohio is the designated authority to grant, suspend, deny, revoke, or limit SAF access. (See AFI 16-701, *Special Access Programs*).

3.10.3. Commanders control security clearances within their activity. See para 7.1.2.

3.10.4. See Chapter 7 for granting of access to classified information.

3.11. Interim Security Clearances. Commanders may grant interim security clearance for Top Secret and Secret access to classified information when the requirements of DOD 5200.2-R, para 3-401 have been met. Consult the DCII and the CAVS to confirm the status of an investigation and ensure there is no disqualifying information prior to granting the interim security clearance. Interim clearances may be revoked at any time based on unfavorable information identified in the course of the investigation.

3.11.1. Interim Top Secret security clearances must be based on all of the following:

3.11.1.1. Favorable ENTNAC, NAC, NACI, NACIC, NACLC, or ANACI completed.

3.11.1.2. Favorable review of EPSQ or SF86.

3.11.1.3. Favorable review of local personnel records, base/security force records, medical records, and other security records, as appropriate.

3.11.1.4. Confirmed receipt of SSBI request at DSS by DSS EPSQ Receipt System available through the DSS web site or at OPM through the supporting CPF.

3.11.2. Interim Secret security clearances must be based on all of the following:

3.11.2.1. Favorable review of EPSQ or SF 86.

3.11.2.2. Favorable review of local personnel records, base/security force records, medical records, and other security records as appropriate.

3.11.2.3. Confirmation of a previous secret security clearance for newly hired civilian employees who have held a secret security clearance as a former military member (without a break in service of 24 months) or who hold a secret security clearance either as an Air Reserve Technician or as a traditional reservist.

3.11.2.4. Confirmed receipt of NACLC request at DSS by DSS EPSQ Receipt System. Confirmed receipt of ANACI request at OPM through the supporting CPF.

3.11.3. Civilians may occupy noncritical-sensitive or critical-sensitive positions pending completion of ANACIs or SSBIs, as appropriate. Commander or staff agency chief (or designee) prepares a waiver of pre-employment investigation requirements when such action is necessary and in the national interest. Interim security clearances may not be granted until after the waiver memorandum is signed.

3.11.4. Interim security clearances must be documented in the CAVS (see para 7.4) or in writing if the CAVS is unavailable until the final security clearance is granted by the CAF.

3.11.4. (8FW) Security Managers (SM) are responsible for updating JPAS to reflect the date the interim clearance was granted by the unit commander. The SM will maintain a copy of the interim clearance authorization letter and forward a copy to Personnel Security Program Manager (8 SFS/SFAIP).

3.12. Access to Classified Information by Non-US Citizens.

3.12.1. Initial Limited Access Authorization (LAA). The MAJCOM/SF approves the request for a personnel security investigation for the purpose of LAA. Approvals are returned to the requester and an information copy is provided to the CAF. Authorized requesters initiate the personnel security action and submit a SSBI to DSS. A favorable SSBI is a prerequisite for LAA. The CAF will adjudicate the SSBI, issue the LAA authorization to MAJCOM/SF, and enter the information in the Adjudi-

cation Management System (AMS). MAJCOM/SF forwards the authorization to the requester. The requester grants the LAA. Requirements governing nondisclosure agreement form and a security termination statement apply to LAAs.

3.12.2. Annual Certification. MAJCOM/SF provides an annual report to the CAF by 1 Nov of each year certifying the continued need for the command's LAAs. The CAF provides a consolidated report to HQ USAF/XOFI by 25 Nov each year. HQ USAF/XOFI approves the report and forwards to OASD(C3I) by 1 Dec of each year.

3.12.3. (8FW) **Access to Classified Information by Non-US Citizens.** All initial and annual Limited Access Authorization's (LAA) will be coordinated through 8 SFS/SFAIP. Commanders review and validate approved LAAs annually.

3.13. Access by Persons Outside the Executive Branch. Refer to AFI 31-401, *Information Security Program Management*, for granting access to persons outside the Executive Branch.

3.13.1. Authorized requesters submit the appropriate investigation according to Atch 2 based on the level of access required.

3.13.1.1. Annotate the request, "Request for investigation is required IAW DOD 5200.1-R, paragraph 6-201, Access to Person Outside the Executive Branch."

3.13.1.2. The CAF does the adjudication and enters the results in the AMS.

3.14. Access by Different Categories of Individuals.

3.14.1. Voluntary Emeritus Corps and Intergovernmental Personnel Act (IPA).

3.14.1.1. There is an affiliation with the Government by virtue of the signing of an agreement. As a general rule, these individuals will not have access to classified information. In certain instances, the commander may approve access to classified information.

3.14.1.2. Access will be justified and must provide a specific benefit or gain to the Government.

3.14.1.3. The access will be commensurate with the level the person held prior to retirement/separation or the level currently held by IPA personnel under the National Industrial Security Program. Offices should accept and maintain visit authorization requests submitted by the sponsoring cleared facility as evidence of an IPA participant's current clearance.

3.14.1.4. Access will be kept to the absolute minimum for the work being performed and limited to a specific time period.

3.14.1.5. The agreement between the individual and the organization will include a security clause.

3.14.1.6. The individual will sign an SF 312, **Classified Information Nondisclosure Agreement (NdA)** and be briefed or re-briefed on security requirements (individuals need not sign another SF 312 if verification can be made that an NdA was previously signed).

3.14.1.7. Physical custody of classified information is not authorized.

3.14.1.8. The CAF will certify the individual's security clearance. If a break in service exceeds 24 months, the requesting organization must initiate a request for the appropriate investigation.

3.14.1.9. The CAF will provide an AF Form 2584, **Record of Personnel Security Investigation and Clearance** to the requesting organization if required due to lack of automation capabilities.

3.14.2. Consultants. A consultant, paid or unpaid, will only require access to classified information at an Air Force activity or in connection with authorized visits and is not required to be cleared under the National Industrial Security Program. The consultant is considered to be an Air Force employee and will be issued a clearance, adjudicated by the CAF, in accordance with this AFI.

3.14.3. Individual Ready Reserve (IRR). The IRR is a manpower pool of pre-trained individuals who have already served in active component units or in the Selected Reserve and have some part of their Military Service Obligation remaining. Refer to DOD 1215.15-H*, Reserve Components of the U.S. Armed Forces*.

3.14.3.1. As a general rule, these individuals will not have access to classified information. In certain instances, the commander may approve access to classified information.

3.14.3.2. Access will be justified and must provide a specific benefit to the Air Force.

3.14.3.3. Access will be commensurate with the level the person held prior to transfer to the IRR, kept to the absolute minimum for the work being performed, and limited to a specific time.

3.14.3.4. An agreement between the individual and the organization is required and will include a security clause.

3.14.3.5. The individual will sign an SF 312, **NdA**, and be briefed or re-briefed on security requirements (individuals need not sign another SF 312 if verification can be made that one was previously signed).

3.15. One Time Access. A general court martial convening authority or equivalent Senior Executive Service member, MAJCOM commander, wing commander, or civilian equivalent may approve access to classified information at a higher level than authorized by the existing security clearance during contingencies, or when an urgent operational or contractual exigency exists. This authority can be used when the conditions of DOD 5200.2-R, para 3-406 are met. This does not apply to SCI access (see para 3.18 below), COMSEC, NATO, or foreign government information. The approving authority's authorization for the access is maintained on file with the servicing security manager and or servicing security activity until the access is no longer needed.

3.16. Processing Requests for Access by Retired General Officers or Civilian Equivalents. An active duty general officer, or Senior Executive Service (SES) member may grant access to a retired general officer, or SES member for a period of 180 days when conditions of DOD 5200.2-R are met. Coordination with servicing security activity is necessary. The access is recorded in the CAVS. A request for a security investigation is not necessary. See AFI 31-401 for guidance on retention of the form. If it is confirmed an SF 312 was signed, it is not necessary for a duplicate signature.

3.17. Processing Requests for Access by Historical Researchers. Refer to AFI 31-401 for guidance in granting of access to researchers.

3.17.1. Authorized requesters request a NAC according to Atch 2. Identify the request as "Special Category Historical Researcher" in remarks.

3.17.2. The CAF will forward the completed investigation to the Air Force Historian.

3.17.3. The United States Air Force History Support Office (AFHSO/HO), 200 McChord, Box 94, Bolling AFB DC 20332, will make the access determination.

3.18. Sensitive Compartmented Information. The Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI), 1480 Air Force Pentagon, Washington DC 20330-1480, controls access to SCI within the Air Force. Routine prescreening for SCI access is no longer required. Refer to AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI).* for specific guidance on conducting SCI prescreening interviews, requesting investigations, granting access, and waiver information.

3.18.1. The 319th Training Squadron (319 TRS/TPCSS), 1550 Wurtsmith Street, Suite 7, Lackland AFB TX 78236-5242, conducts interviews pertaining to individuals identified for SCI positions during basic military training. They also conduct interviews of individuals requiring Top Secret for Air Force specialty code retention and critical personnel reliability program certification.

3.18.2. A single agency check (SAC) is required on the following categories of individuals associated with the subject of an SSBI (a) spouse or cohabitant, (b) immediate family members, 18 years old or older, who were born outside the United States. If marriage or cohabitation occurs after completion of the SSBI, submit Spouse SAC via EPSQ to DSS. Keep one copy for the authorized requester's suspense file.

3.19. Single Integrated Operational Plan-Extremely Sensitive Information. See AFI 10-1102, *Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).*

3.20. Presidential Support Activities. The following guidance supplements DOD Directive 5210.55, Department of Defense PSP and DOD Instruction 5210.87, Selection of DOD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs). The PSP includes personnel assigned duties involving regular or frequent contact with or access to the President or Presidential facilities, communications activities, or modes of transportation.

3.20.1. The Office of the Administrative Assistant, Director for Security and Investigative Programs (SAF/AAZ) is the single office designated to develop policy and represent the Air Force on matters covered by the DOD Presidential Support Directive and Instruction.

3.20.2. HQ USAF/XOFI implements policy for the PSP.

3.20.3. The CAF:

3.20.3.1. Manages adjudicative functions as required by the PSP.

3.20.3.2. Accomplishes requisite cover letters and coordination with support units on behalf of SAF/AAZ.

3.20.3.3. Forwards nomination packages, regardless of adjudicative outcome to SAF/AAZ.

3.20.3.4. Submits the "Information Requirements" report on a quarterly basis to SAF/AAZ for approval and forwards approved report to the Executive Secretary. Copies of the approved report are provided to HQ USAF/XOFI, the servicing security activity, and contracting officers for distribution.

3.20.3.5. Maintains historical files.

3.20.4. SAF/AAZ advises commanders or company representatives when nominees have been selected or nonselected by SAF/AAZ or the Executive Secretary. SAF/AAZ enters selection status information in the AMS.

3.20.5. Appeals. Any DOD civilian or contractor employee not selected for, or removed from, presidential support duties shall be afforded an opportunity to appeal this decision as provided in DODD 5210.55 and DODI 5210.87. The governing directives do not provide appeal rights for military members, however, when exceptional mitigating circumstances exist, or derogatory information is reported in error, SAF/AAZ will reconsider non-selection decisions. Reconsideration of military non-selections requires unit commander approval and involvement.

3.20.6. The servicing security activity of the nominating unit:

3.20.6.1. Processes the appropriate investigation to DSS or OPM. See Atch 2.

3.20.6.1.1. Completes DD Form 1879 for an SSBI by typing "YANKEE WHITE" in capital letters in the remarks section. Checks the "Presidential Support" block and indicates the level of clearance required for the position. Includes the title of the authorized presidential support position and the unit or organization to which the individual will be assigned.

3.20.6.1.2. Completes the SF 86 for a NACLC by typing "YANKEE WHITE" in capital letters in the remarks section. Type "Presidential Support" and indicate the level of clearance required for the position. Include the title of the authorized presidential support position and the unit or organization to which the individual will be assigned.

3.20.6.2. Prepares the "servicing security activity" nomination memorandum for the CAF outlined in Atch 9.

3.20.6.3. Forwards the nomination memorandum to the CAF for further processing.

3.20.6.4. Notifies the servicing medical facility that must mark and monitor the individual's medical records, upon notification by the Commander that the member has been approved for presidential support duties. See Atch 10.

3.20.6.5. Notifies the servicing medical facility when individuals are no longer assigned presidential support duties.

3.20.6.6. Notifies the CAF presidential support representative telephonically within 24 hours when an individual's access has been temporarily suspended or removed and note if publicity is anticipated. The temporary suspension or removal should also be input into the CAVS which will provide the information to the CAF electronically. Provides written follow-up to include a summary of all available information within 2 working days. If applicable a full report of investigation of the allegations and commander's recommendation for removal or reinstatement shall be forwarded to the CAF within 50 days. Provide a status report within 30 working days. Temporary suspension in which the issues are unresolved by the applicant within 90 days shall become a permanent removal. Notifies the CAF within five working days, when this occurs. Notifies the CAF when individual's (1) are permanently removed from presidential support duties, (2) separate or (3) retire. The CAF notifies SAF/AAZ immediately in all cases.

3.20.6.7. Completes and forwards to DSS the FD Form 258, **FBI Fingerprint Card.**

3.20.6.8. Forwards requests for transfer or designation of additional presidential support positions to the CAF for coordination. The CAF will attach the current unit billet structure and forward it to SAF/AA for approval.

3.20.6.9. Processes individuals for periodic reinvestigations.

3.20.7. Servicing Medical Authority:

3.20.7.1. Ensures the medical records of members approved for presidential support duties are identified, evaluated and monitored while assigned to presidential support.

3.20.7.2. Identifies the medical records using AF Form 745, **Sensitive Duties Program Record Identifier** (see AFI 41-210, *Patient Administration Functions*).

3.20.7.3. Immediately notifies the individual's commander or designated representative and the servicing security activity when a significant effect on the individual's suitability to perform presidential support duties is expected as a result of medical, dental, or mental health treatment or medication , and if drug or alcohol abuse is suspected.

3.20.7.4. Provides a summary of pertinent health records to individual's commander or designated representative at their request. The actual record will be provided only if specifically requested for clarification purposes or other compelling need. Mental health clinic records may, if necessary, be reviewed in their entirety by the individual's commander or reviewing official, provided a privileged mental health provider is present to help interpret psychological testing data and other technical information which may be contained in the record. The information contained in the record is protected under the Privacy Act and is not to be discussed or released except as indicated in this paragraph.

3.20.8. Commander and or Supervisory Indoctrination Program. Commanders and or supervisors will become knowledgeable of DOD 55210.55 and requirements of this AFI prior to evaluating and recommending individuals for presidential support positions.

3.20.9. Continuing Evaluation. Commanders and supervisors continually evaluate the trustworthiness of personnel serving in presidential support duties to ensure they meet the standards. Take necessary action when adverse information becomes known to access the validity of the information. If appropriate, initiate action for suspension and or removal. Follow SIF procedures as outlined in Chapter 8 when unfavorable information surfaces on an individual already in the PSP program.

3.20.10. Investigative Requirements. Persons nominated for presidential support duties must have an SSBI or NACLC current within 36 months of assignment to presidential support duties. The DD Form 1879/SF 86 will be annotated to reflect if the investigation is for initial assignment into the program.

3.21. Nuclear Weapons Personnel Reliability Program. Refer to AFI 36-2104, *Nuclear Weapons Personnel Reliability Program (PRP)* for PRP certification and investigative guidance. A new personnel security investigation (PSI) or periodic reinvestigation is required when there is a break in personnel reliability program certification of more than five years, or for new PRP assignments when the security investigation date is over five years. A new PSI is also required any time a break in service of more than 24 months occurs between completion of the security investigation and PRP certification dates.

3.21.1. (8FW) **Nuclear Weapons Personnel Reliability Program.** Personnel requiring a security clearance update for an upcoming Personnel Reliability Program (PRP) assignment, must obtain a

security requirement letter from 8thMission Support Squadron, Relocations and Employment Flight, Assignments (8MSS/DPMAR) stating the type of clearance required. This letter must be brought to 8 SFS/SFAIP along with the other clearance material prior to submission to the investigating agency.

3.22. Access to North Atlantic Treaty Organization Classified Information. U.S. military personnel, civilians, and contractors shall be permitted temporary access to COSMIC Top Secret information based on a final U.S. Secret clearance and issuance of an interim Top Secret clearance, pending completion of an SSBI and issuance of a final Top Secret clearance. The temporary access will be valid until completion of the investigation and adjudication of the final clearance. However, the agency granting the access will rescind it if adjudicatively significant information is identified during the course of the investigation. The same procedures apply to personnel not assigned to a NATO staff position, but requiring access to NATO COSMIC Top Secret, Secret or Confidential information. The granting agency records NATO access in the CAVS. Refer to AFI 31-406***, Applying NATO Protection Standards***.

3.23. Special Access Program. Certain programs require additional investigative and or safeguarding requirements. Refer to AFI 16-701, *The US Air Force Special Access Programs*.

3.24. Processing Requests for Access to Restricted Areas, Sensitive Information or Equipment Not Involving Access to Classified Information. Access for unescorted entry may be granted based on the following investigative requirements. Refer to Atch 3, table A3.6.

3.24.1. DOD and OPM civilians require a National Agency Check with Written Inquiries and Credit Check (NACIC).

3.24.2. Air Reserve forces personnel with a current Entrance National Agency Check (ENTNAC) or NAC may have unescorted entry to restricted areas while in civilian status, pending completion of the required NACIC.

3.24.3. Department of Energy employees require an “L” (Secret) clearance.

3.24.4. Federal employees require a NAC.

3.24.5. United States active duty, retired, or separated military members with an Honorable Discharge and no break in service greater than 24 months, may use a previously completed ENTNAC or NACLC.

3.24.6. Contractor employees require a NAC. Contractors operating as visitor groups only (contract performance exceeding 90 consecutive days), have the following option. Commanders may grant individuals access to restricted areas subject to: (1) the contractor completing the SF 85P and it is submitted to OPM for a NAC; (2) a check of the Defense Clearance and Investigations Index reveals no relevant, significant information which might preclude unescorted access; and (3) a check of appropriate local records.

3.24.7. Commanders may waive on a case by case basis, the investigative requirements for unescorted entry to restricted areas containing PL2 and or 3 resources pending completion of a favorable NAC, or NACIC after favorable review of the completed personnel security questionnaire for the investigation. Decisions to deny or withdraw must be fully supported by the documented facts. Individuals must be informed of the adverse information about them (unless precluded by security considerations) and given the opportunity to appear before the commander. This allows the individual to

refute or to mitigate the information. Forward appeals of denials or withdrawals to the MAJCOM commander or designee.

3.24.8. Interim access to restricted areas may be granted to military, civilians, and contractors. Use the same procedures for interim access as established for interim AIS (para 3.27).

3.24.9. For Foreign National military members and host military members assigned to USAF activities, entry authorization is based on government-to-government agreements, treaties, and unified command directives. A SSBI is required for restricted areas containing PL1 or 2 resources, and a local agency check for restricted areas containing PL3 resources.

3.24.10. Unit commanders through the installation commander, request NACs on contractor employees requiring unescorted entry to restricted areas. The CAF adjudicates the completed NAC and enters the results in the appropriate database. Installation commanders approve all denials or withdrawals of unescorted entry for contractor employees.

3.25. Nonappropriated Fund Employees. Human Resources Office (HRO) managers (Atch 4) designate positions of trust. AFPD 34-3, *Nonappropriated Funds Personnel Management and Administration* and AFI 34-301, *Nonappropriated Fund Personnel Management and Administration* establish policies for the management of the AF Nonappropriated Fund Personnel Program. HRO managers make suitability determinations according to the suitability criteria outlined in 5 CFR 731.201-202. The determination will be filed in the individual's personnel file.

3.26. Special Agents and Investigative Support Personnel. See Atch 3. Non-investigative personnel whose official duties require direct investigative support include administrative processing and or handling of the investigative reports on a continuous basis. The CAF adjudicates the investigation and enters the data in the DCII and AMS.

3.27. Personnel Occupying Information Systems Positions Designated Auto mated Information Systems, AIS-I, AIS-II, and AIS-III (formerly ADP positions). Refer to DOD 5200.2-R, appendix K for ADP definitions.

3.27.1. See Atch 3 for AIS I, II, and III investigation requirements. See paragraph 3.11 for interim security clearance requirements.

3.27.2. The CAF provides the results of the investigations for AIS I, II, and III purposes to the authorized requester for the commander's suitability determination according to the suitability criteria outlined in 5 CFR 731.201-202. The CAF does not review the investigation for security clearance purposes.

3.27.3. Commanders may recommend to the Designated Approving Authority (DAA) that interim AIS access be granted. Commanders may waive, on a case by case basis, the investigative requirements for access to AIS pending completion of a favorable ENTNAC, NAC, NACIC, ANACI, or SSBI, after favorable review of the completed personnel security questionnaire for the investigation. Commanders confirm that the following actions have been accomplished prior to access:

3.27.3.1. Mandatory information assurance training has been given and documentation by a supervisor accompanies the request.

3.27.3.2. Systems Administrators have implemented measures to limit access to the information required to conduct assigned duties.

3.27.3.3. Commanders and or supervisors have ensured increased monitoring of the individual having AIS access.

3.27.3.4. For military members: after verification from the unit security manager that the required investigation has been initiated and the preliminary suitability determination has been made.

3.27.3.5. For AF Appropriated and NAF Civilians (over 180 day appointment or an aggregate of 180 days has been reached):

3.27.3.5.1. CPF/HRO returns to the commander, a favorable suitability determination based on the results of the completed OF 306, Declaration for Federal Employment, and the SF 85, Questionnaire for Non Sensitive Positions, or 85P.

3.27.3.5.2. Unit security managers initiate a local files check (LFC).

3.27.3.5.3. Security Forces verify that the appropriate investigation has been initiated and no adverse information was revealed in the completed LFC.

3.27.3.6. For AF Appropriated and NAF Seasonal or Summer Hire Employee (under 180 day appointment):

3.27.3.6.1. CPF/HRO returns to the commander, a favorable suitability determination based on the results of the completed OF 306.

3.27.3.6.2. Unit security managers initiate a LFC.

3.27.3.6.3. Security Forces verify that no adverse information was revealed in the completed LFC.

3.27.3.7. For Contractors:

3.27.3.7.1. Unit security managers initiate the LFC.

3.27.3.7.2. Security Forces verify that the appropriate investigation has been initiated and no adverse information was revealed in the completed LFC.

3.28. Periodic Reinvestigations. Authorized requesters submit requests for PRs in the following order based on the individual's access and duties. Use the following criteria for prioritizing cases: PRP, Presidential Support, NATO, and other special access programs, as determined by the commander. See Atch 3 for periodic reinvestigation requirements.

Chapter 4

RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

4.1. Prior Federal Civilian Investigations. Investigations previously conducted on civilian employees are suitable and accepted for granting immediate access to classified information.

4.1.1. Civilian Personnel Flight:

4.1.1.1. Verifies prior federal employment in a sensitive position was continuous with no single break longer than 24 months.

4.1.1.2. Confirms the individual is employed in a sensitive position with the Air Force and that clearance eligibility is valid.

4.1.1.3. Confirms with the CAF that a valid investigation is on file. The CAF updates the DCII and AMS.

4.1.1.4. Forwards verification of the investigation to the subject's commander.

4.1.2. Unit commander:

4.1.2.1. Grants access when actions are completed.

4.1.2.2. Destroys all copies of the documentation when SK shows the security clearance data.

Chapter 5

REQUESTING PERSONNEL SECURITY INVESTIGATIONS

5.1. General.

5.1.1. Security Managers provide personnel security support to active duty military, civilian, and guard and reserve members assigned or attached to the active duty organization.

5.1.1.1. Submit completed personnel security questionnaires to supporting authorized requester. See Atch 3 for additional guidance.

5.1.1.2. (Added-8FW) . The latest version of the Electronic Personnel Security Questionnaire (EPSQ) will be used when submitting requests for personnel security investigations.

5.2. Authorized Requesters.

5.2.1. MAJCOM, field operating agency (FOA), or direct reporting unit (DRU) staffs designate authorized requesters to initiate PSIs for their organization. As a general rule, the number of authorized requesters should be kept to a minimum; one authorized requester to support a base. However, additional authorized requesters can be designated. Submit requests for authorized requester codes through ISPM channels to HQ USAF/XOFI. Provide justification for the need to be an authorized requester and include PASCODE.

5.2.2. Authorized requesters, through their MAJCOM, provide the CAF with the name, telephone number, and office symbol of individual(s) who may obtain security clearance and or investigative data on individuals within their organization.

5.2.3. Authorized requesters may query the CAVS or call the CAF Customer Support Division at DSN 754-1242/43 to determine investigative and or adjudicative status.

5.2.4. Authorized requesters approve and submit personnel security questionnaires to DSS and OPM according to Atch 2.

5.2.5. Advise HQ USAF/XOFI when authorized requesters are disestablished.

5.3. Criteria for Requesting Investigations. See Atch 3 for the type of investigation to request.

5.4. Request Procedures. See Atch 2 for the request procedures.

5.4.1. (Added-8FW) . SMs will complete each individual's AF Form 2583, *Request for Personnel Security Action*. AF Form 2583s submitted to 8 SFS/SFAIP must be reacomplished if the signatures by the SM and 8th Medical Operations Squadron, Flight Medicine (8 MDOS/SGOAF) personnel exceed 30 days.

5.4.2. (Added-8FW) . Personnel, who are not Security Access Requirement (SAR) coded at Kunsan AB and require a periodic reinvestigation or clearance upgrade for an upcoming assignment, must obtain a security requirement letter from 8 MSS/DPMAR stating the type clearance required. This letter must be brought to 8 SFS/SFAIP along with the other clearance material prior to submission to the investigating agency.

5.5. Priority Requests. ISPMs submit, through their MAJCOM, requests with justification for priority handling to HQ USAF/XOFI for approval.

5.6. Personal Data Provided by the Subject of the Investigation.

5.6.1. The Air Force goal for processing personnel security investigation requests at base level is 14 duty days. However, commands that have extensive deployments and TDY requirements may establish their own internal management controls and or timelines for the processing of investigation requests.

5.6.1.1. (Added-8FW) . Personnel Security Investigations (PSI) will be submitted within 30 days of notification from the unit SM. SMs are responsible for tracking the date the individual was notified. ***NOTE:*** Failure to provide the PSI within the above timeframe is grounds for Security Information File (SIF) establishment.

5.6.2. The subject of the investigation will provide the required documentation to the security manager to verify birth and education information. See Atch 2 for details.

5.6.3. Individual Mobilization Augmentee (IMA): Upon accession, IMAs complete the PSI during the first three days of the individual duty training (IDT) period or not later than 90 days at the unit of assignment or attachment and turn-in to the servicing security manager and or gaining active duty security manager.

5.6.4. See Chapter 8 for actions when individuals refuse to provide the required information for a personnel security investigation.

5.6.5. DSS and OPM are the DOD repository of personnel security investigative files. To obtain a personal copy of an investigation, forward a notarized request that includes: name, SSAN, date of birth, and place of birth to: DSS, ATTN: Privacy Act Office, PO Box 46060, Baltimore, MD 21240-6060 or OPM, ATTN: FOIA, PO Box 618, 1137 Branchton Rd, Boyers, PA 16018-0618. The request should refer to the Privacy Act and include a valid return address. All signatures must be notarized. Military personnel may use a commissioned officer in lieu of a notary public to attest to the signature. Identify the SSN and rank of the officer. Also refer to AFI 33-332, *Air Force Privacy Act Program*.

Chapter 6

ADJUDICATION

6.1. Central Adjudication Authority. The 497 IG/INS, Air Force Central Adjudication Facility (CAF) is the Central Adjudication Authority.

6.1.1. The policy and criteria set forth in DOD Regulation 5200.2-R, paragraph 2-200, 6-102 and Appendix I will be applied in making personnel security determinations for a security clearance or assignment to sensitive duties.

6.1.2. Unfavorable adjudication results in the denial/revocation of clearance eligibility (see Chapter 8).

6.1.3. The CAF will review all investigative products and make an eligibility determination.

6.2. Adjudicative Record. Personnel security determinations are reflected in SK (see para 7.4).

Chapter 7

ISSUING CLEARANCE AND GRANTING ACCESS

7.1. General.

7.1.1. The 497 Intelligence Group/INS, Directorate of Security and Communications Management, HQ AIA, the Air Force Central Adjudication Facility, is the designated authority to grant, suspend, deny, or revoke personnel security clearances and SCI accesses (see Chapter 11).

7.1.2. Position Designations (7-100c). Commanders:

7.1.2.1. Determine the level of access necessary for each military and civilian position based on mission needs. Each position is coded with the appropriate security access requirement (SAR) and identified in the unit manning document (UMD), the Defense Civilian Personnel Data System (DCPDS), and SK. See Atch 3, for SAR code definitions. If the SAR code requires a change, the unit commander submits an authorization change request to the servicing security activity.

7.1.2.2. Conduct a review annually to determine the accuracy of position coding, eliminate unnecessary access codings, and adjust SAR code appropriately.

7.1.2.2. (8FW) Commanders review the unit SAR code listing annually to ensure accuracy and provide a written response of completion to 8 SFS/SFAIP NLT 31 December of each year. Submit all SAR code position change requests utilizing a Manpower Authorization Change Request Letter, through 8 SFS/SFAIP. A sample letter is located in the Security Manager Handbook.

7.1.2.3. Record findings in the UMD and SK.

7.1.2.4. Ensure only necessary investigations are requested to meet mission essential needs.

7.2. Investigative Requirements for Air Force Specialty Codes. HQ USAF/XOFI reviews, evaluates, and approves requests for adding security clearances or investigations as AFSC prerequisites.

7.2.1. Mandatory Secret or Top Secret requirement may be authorized when 100 percent of the authorizations in the AFSC are coded in the UMD as requiring access to classified information.

7.2.2. Mandatory Secret or Top Secret requirement may be required when every position in a specialty is not coded as requiring access to classified information if the functional community can validate security access requirements for the AFSC and provide justification that demonstrates mandatory qualification required for mission accomplishment, such as access to classified information or equipment.

7.3. Issuing Security Clearance. The CAF issues security clearance eligibility. Security clearance eligibility determination is entered in the DCII and AMS (see para 7.4).

7.3.1. Security clearance data can be verified by the CAVS, Permanent Change of Station Orders, or Temporary Duty Orders.

7.4. SENTINEL KEY. SK is the Air Force personnel security automated system that contains investigative and clearance data. It consists of two applications, the Adjudication Management System (AMS) and the Clearance and Access Verification System (CAVS). SK will provide a two-way data flow between the CAF and the authorized users at the base. SK replaces the PC III generated ASCAS rosters. SK is the Air

Force system of records for clearance eligibility and access information. SK allows communication between the CAF and its customers. All information in SK is unclassified, but must be protected according to the requirements for privacy/sensitive information and for official use only (FOUO) in accordance with AFI 33-332, *Air Force Privacy Act Program* and DODR 5400.7/AF Supplement, *DOD Freedom of Information Act Program*.

7.4.1. AMS is the application used by the CAF and is restricted to CAF personnel only.

7.4.1.1. It is a centralized database enabling CAF personnel to post adjudication results; security clearance determinations; access eligibility; pending actions; status of due process actions, i.e. security information files; statistical reporting requirements; and other personnel security management functions.

7.4.1.2. Selected data fields from AMS will be available through CAVS to Air Force customers/users almost immediately after input by CAF personnel and within 24 hours of data input by other customers/users.

7.4.2. CAVS is the application used by MAJCOM/FOA/DRUs, ISPMs, SSOs, unit level security managers, and other individuals with personnel/physical security responsibilities. MAJCOM/FOA/DRUs will determine those organizations and individuals within their organizations who will be given CAVS access. Clearance data elements in the CAVS include the full date and type of investigation and the full date and status of security clearance. The information is invalid when any of these four data elements are incomplete.

7.4.2.1. Use the most current highest level eligibility recorded in the CAVS when more than one entry appears for an individual.

7.4.2.2. An individual may have multiple SAR codes recorded in the CAVS if the individual is in multiple positions (i.e. civilian, reserve, or air national guard). The level of access given to the individual should be based on the access necessary for the position. Commanders make the decision on the level of access required.

7.4.2.3. The term "DCID 6/4 (formerly DCID 1/14)" means the person has been the subject of a SSBI, has been granted a Top Secret security clearance, is eligible for SCI access if required for mission essential purposes (depending on the currency of the investigation) and or may already have SCI access. See AFMAN 14-304.

7.4.2.4. The CAVS will provide the following information:

7.4.2.4.1. An individual's security clearance level and access.

7.4.2.4.2. Visit and suspension notifications.

7.4.2.4.3. SCI indoctrination, nondisclosure statement, and debriefing dates.

7.4.2.4.4. Establishment of a SIF.

7.4.2.5. Access to the CAVS is restricted to Air Force employees only. Contractors and others who are assigned to an ISPM or SSO office must have prior approval by the SK Program Management Office (497 IG/INSP (PMO)) for access.

7.4.2.6. There are 7 User Levels in the CAVS. These levels are defined as follows:

7.4.2.6.1. Level 1: CAF personnel and Systems Administrators.

7.4.2.6.2. Level 2: MAJCOM/FOA/DRU SCI security personnel.

7.4.2.6.3. Level 3: Base SCI security personnel.

7.4.2.6.4. Level 4: MAJCOM/FOA/DRU non-SCI security personnel.

7.4.2.6.5. Level 5: Base ISPM security personnel.

7.4.2.6.6. Level 6: Entry Controller.

7.4.2.6.7. Level 7: Unit Level Security Manager.

7.4.2.7. User Levels have the following CAVS read and write access:

7.4.2.7.1. User levels 2-7 have read access to all Air Force personnel.

7.4.2.7.2. User levels 2 and 4 may write to records within their MAJCOM/FOA/DRU PASCODE.

7.4.2.7.3. User levels 3 and 5 may write to records within their local PASCODE and to records of individuals assigned to another MAJCOM/FOA/DRU supported by levels 3 and 5.

7.4.2.7.4. User level 6, entry controller, has the ability to verify an individual's clearance eligibility and access in the CAVS. MAJCOM/FOA/DRU may have reports printed for entry controllers by base ISPM security personnel (user level 5) listing the clearance eligibility and access of expected visitors. Reports will only be valid for the date and time printed.

7.4.2.7.5. User level 7 has the ability to write non-SCI access (interim, secret, and top secret); nondisclosure dates; NATO access; and the indoctrination/debriefing dates. Level 7 is also authorized to view non-SCI access history and print reports associated with their write capabilities.

7.4.2.7.5. (8FW) SMs will provide 8 SFS/SFAIP with a roster identifying all personnel who require a periodic reinvestigation or upgrade NLT the first of every month. SMs will utilize this list to track the unit backlog.

7.4.2.8. ISPMs determine the number of users and the access level for each user within their command. The system administrator will establish user accounts. SK allows unlimited users on one computer, but each user must have an individual account. A user account must be restricted to the registered user only.

7.4.2.9. User Levels 1-3 must have a Top Secret clearance based on an SSBI or PR. User Levels 4-7 require a Secret clearance based on an ENTNAC, NAC, NACLC, NACI, NACIC, or ANACI.

7.4.3. The CAF will publish and keep current a SK training guide with instructions on the use of AMS and CAVS. The CAF will review/update the SK web page at least monthly, to provide additional guidance and references as needed.

7.4.4. Requests for changes to SK must be forwarded by the MAJCOM/FOA/DRU Security Forces or Special Security Office (SSO) to the SK Requirements Group through the 497 IG/INSP, 229 Brookley Ave, Bolling AFB DC, 20332-7040.

7.4.5. SK will be replaced with the Joint Personnel Adjudication System (JPAS) which will be the DOD personnel security automated system that contains investigative and security clearance data.

7.5. Granting Access. Commanders grant access to classified information when required for mission essential needs and only when the following prerequisites are met: (1) individual has the appropriate security clearance eligibility; (2) individual signed an SF 312 (see AFI 31-401); and (3) individual has a need-to-know. Authorized base level users should record access in the CAVS, including NATO and SIOP. See Chapter 3 for other situations when access to classified information may be granted.

7.5. (8FW) Granting Access. SMs, using the JPAS program, will maintain a printed copy of the current month Clearance and Access Verification System (CAVS) roster. The CAVS will be used to verify security clearances before granting access to classified material.

7.5.1. (Added-8FW) . SMs will use JPAS to verify unit personnel have signed a Non- disclosure Agreement (NDA), SF Form 312, *Classified Information Nondisclosure Agreement*. SMs are responsible for updating signed NDA's in SK and mailing them to the applicable address listed in AFI 31-401, *Information Security Program Management,* paragraph 5.5.

7.6. Obtaining Information from the CAF.

7.6.1. Authorized requesters may call the CAF Customer Support Division at DSN 754-1243/42. In situations where no security clearance data is available at the unit, no information is available in the CAVS, and the CAF has valid security clearance information on file, a record of the call will be used as evidence of valid clearance data pending update of the CAVS. The authorized requester prepares a memorandum for record (MFR) showing: (1) name, grade, and organization of the individual calling the CAF; (2) name, grade, organization, and SSN of the subject; (3) name of person at the CAF providing clearance data, and (4) type and date of investigation and, if granted, level and date of security clearance.

7.6.1.1. The authorized requester forwards a copy of the MFR to the individual's security manager.

7.6.1.2. The authorized requester and the unit keep the MFR until the CAVS shows a final security clearance.

Chapter 8

UNFAVORABLE ADMINISTRATIVE ACTIONS

8.1. Referral for Action.

8.1.1. Security Information File (SIF). A SIF is a collection of documents generated as a result of the discovery or development of unfavorable information which brings into question a person's continuing eligibility for a security clearance or access to SCI. It may be established by a commander, civilian equivalent, or by the CAF. The SIF serves as a repository for unfavorable or derogatory information that requires further review, evaluation, or investigation to resolve outstanding administrative or adjudicative concerns. Report administrative change of status information for individuals with SCI access according to AFMAN 14-304.

8.2. Suspension.

8.2.1. Commander:

8.2.1.1. Reviews unfavorable information on individuals under the commander's jurisdiction when reported or developed which would directly impact an individual's security clearance or SCI access, to include the following (see Atch 11 for sample memorandum):

8.2.1.1.1. Activities' tenant or geographically separated units.

8.2.1.1.2. TDY personnel.

8.2.1.2. Establishes a SIF when an individual's activity, conduct or behavior is inconsistent with the security criteria specified in DOD 5200.2-R, para 2-200 and Appendix I. See Atch 12 for sample request for SIF establishment to the servicing security activity.

8.2.1.3. Determines whether or not to establish a SIF on a case by case basis, normally within 20 days of receipt of unfavorable information (as soon as possible if SCI access is involved). This decision is made by considering the seriousness of the incident; the individual's motivation; whether it was out of character for the individual; or whether the undesirable conduct or behavior is likely to continue. Coordination and consultation with the chief of the servicing security activity, SSO (for SCI access) or program security officer (for SAP access) and legal representatives is recommended. However, if the commander has sufficient reason to doubt the validity of unfavorable information the decision to establish a SIF and notification to the CAF may be extended up to 45 days. If the servicing security activity and the commander disagree on establishment of a SIF, elevate the issue to the installation commander for resolution. Once a SIF is formally established it must be processed accordingly and only the CAF has closure authority.

8.2.1.3.1. Examples of reasons to establish a SIF are outlined in para 2-200, DOD 5200.2-R and include the following:

8.2.1.3.1.1. Refusal to sign a required SF 312 or other nondisclosure agreement.

8.2.1.3.1.2. Refusal or intentional failure of an individual requiring an investigation or periodic reinvestigation to provide the personnel security questionnaire information or release statements for review of medical, financial, or employment records.

8.2.1.3.1.3. Refusal by an individual to be interviewed in connection with a personnel security investigation, regardless of whether the information is requested by the investigative agency or the CAF.

8.2.1.3.1.4. Incidents of theft, embezzlement, child or spouse abuse, unauthorized sale or use of firearms, explosives, or dangerous weapons, or misuse or improper disposition of government property or other unlawful activities.

8.2.1.3.1.5. Information leading to permanent decertification from PRP for other than physical reasons.

8.2.1.3.2. The following are some examples of reasons that may not warrant establishment of a SIF:

8.2.1.3.2.1. Minor traffic violations.

8.2.1.3.2.2. Minor one-time alcohol related incident.

8.2.1.3.2.3. Permanent decertification from PRP related to medical reasons of a physical nature.

8.2.1.3.2.4. Disciplinary issues; such as failure to repair; poor duty performance; failure to maintain weight standards; and any single isolated incident of poor judgment based on immaturity or extenuating circumstances which does not impact on the individual's ability to safeguard classified information.

8.2.1.3.2.5. Federal civilian employees occupying nonsensitive positions.

8.2.1.3.2.6. Incidents where a SIF has already been established by the CAF based on the same unfavorable information.

8.2.1.4. Determines whether or not to initiate suspension action for the individual's access to classified information upon establishment of a SIF. If the decision is to suspend the person's access to classified information the same decision automatically applies to the SCI and SAP access. The access to classified information and SCI is considered one under the new DOD personnel security common adjudicative guidelines. Additionally, the commander determines suspension of unescorted entry to restricted areas if applicable. The determination to suspend should be based on a thorough review of the facts and an assessment of the risk to national security**.** For SCI access see AFMAN 14-304 and DOD S-5105.21-M-1*, Sensitive Compartmented Information Administrative Manual***.**

8.2.1.5. Notifies the individual accordingly with information copy to the servicing security activity. See Atch 13 and 14 for sample memorandums.

8.2.1.6. Requests AFOSI investigation, if criminal activity is involved.

8.2.1.7. Includes a recommendation whether to grant, reinstate, deny, or revoke the individual's security clearance and or SCI/SAP access and the rationale for the decision in the completed SIF. The documented facts must fully support the recommendation. Refer to DOD 5200.2-R, Appendix I, Adjudicative Guidelines.

8.2.1.8. Requests the CAF to *immediately* close a SIF favorably via priority message (through the MAJCOM or activity SSO for SCI) when special circumstances exist (i.e., individual was falsely accused or holds a special expertise that is essential for mission accomplishment). The com-

mander provides the CAF with the SIF (if not already at the CAF) and full justification for favorable closure. The CAF will then make the security clearance determination or request additional information, if necessary.

8.2.1.9. Endorses requests by Chief of Servicing Security Activity (SF), SSO, and Program Security Officer (PSO) for evaluations and relevant documentation from on base activities when issues warrant such coordination.

8.2.2. Chief of Servicing Security Activity, SSO, and PSO:

8.2.2.1. Provides guidance to commanders on SIF establishment. SF is OPR for Top Secret and Secret security clearance SIFs; SSO is OPR for SCI access SIFs.

8.2.2.2. Establishes, processes, maintains, monitors SIFs for commanders. See Atch 15 for sample memorandum for notification to the commander of SIF establishment. See Atch 16 for sample SIF custodian checklist.

8.2.2.3. Provides initial notification to the CAF upon SIF establishment via message or CAVS within 10 days. Provide full name, SSAN, security clearance data, date SIF established, reason, and if access to classified information and SCI has been suspended or withdrawn. If the individual has or is being processed for SCI access, forward the notification to the CAF through the MAJCOM or activity SSO. Notify the CAF via memorandum when the individual will be permitted to continue access to classified information and SCI access. See Atch 17 for sample memorandum. Notify the CAF via memorandum when the individual's access is withdrawn. Process SIFs concerning SCI access according to AFMAN 14-304. If SCI access is involved, the SSO is responsible for managing the SIF in its entirety to include actions required for the security clearance. SF, SSO, and PSO exchange notification information and coordinate actions with each other. Additionally, notify the CAF when:

8.2.2.3.1. Unfavorable information results in a discharge, retirement, or separation. Forward a copy of the discharge or separation orders or a copy of the SF 50B3PT, Notification of Personnel Action, plus any additional unfavorable information used in these actions. If discharge is involved and the individual is or has been indoctrinated for SCI in the past three years, see AFMAN 14-304 for discharge for cause procedures.

8.2.2.3.2. An adverse discharge is overturned and the individual returns to active duty.

8.2.2.4. Notifies the Installation Commander when SIFs are established. See Atch 18 for sample memorandum.

8.2.2.5. Requests evaluations and relevant documentation from the following activities when the issue involved indicates coordination is appropriate (see Atch 19):

8.2.2.5. (8FW) 8 MDOS Counseling Services/Substance Abuse, (8 MDOS/SGOFH) and 8 FW Military Justice (8 FW/JAM) will provide 8 SFS/SFAIP with a monthly listing of personnel whose activity, conduct, or behavior is inconsistent with security criteria specified in DOD 5200.2, *DoD Personnel Security Program,* para 2-200 and Appendix I. This information will be utilized to assist the unit commanders in determining if a SIF needs to be established.

8.2.2.5.1. Director of Personnel. For any Unfavorable Information Files (UIF), performance report summaries, suitability determinations, and personnel actions.

8.2.2.5.2. Security Forces. For any criminal activities or other pertinent data regarding the subject's police record, involvement in previous compromises or security incidents.

8.2.2.5.3. Judge Advocate. For any court proceedings or nonjudicial punishment if legally supportable by nature of individual's actions. For suitability determinations and legal advice, when needed.

8.2.2.5.4. Surgeon General. For any physical, mental, or emotional evaluation that may affect the subject's ability to protect classified information.

8.2.2.5.5. Mental Health Clinic. For any reports of involvement, previous or present, with alcohol or dangerous drugs which may indicate security weakness.

8.2.2.6. Forwards SIF to the gaining servicing security activity or SSO when an individual transfers to another assignment. See Atch 20 for sample memorandum.

8.2.2.7. Forwards completed SIF, with required documentation, to the CAF for closure within 120 days. See Atch 21 for sample memorandum. If SCI access is involved forward the SIF through the MAJCOM or activity SSO to the CAF**.** See AFMAN 14-304 and DOD S-5105.21-M-1 for SCI guidance**.** Refer to DOD 5200.2-R, Chapter 8-102d regarding suspension cases over 180 days. Use first class mail in accordance with DODM 4525-8AFSUP1, *Official Mail Manual*.

8.2.2.8. Contacts the CAF for an extension if SIF cannot be closed in 120 days.

8.2.2.9. Ensures all supporting documentation is included prior to submitting to the CAF. The commander's recommendation and rationale for the final decision must also be included. The following are examples of the types of required documentation relevant to the issue:

8.2.2.9.1. PSIs conducted by DSS, OPM, or similar agencies.

8.2.2.9.2. AFOSI reports of investigation, civil, police, or child advocacy reports.

8.2.2.9.3. Security forces incident or complaint reports and SSO reports.

8.2.2.9.4. Summaries of facts to substantiate any unfavorable information not covered by one of the investigative sources above. Include a complete reference to the source of the information.

8.2.2.9.5. Summaries of UIF entries.

8.2.2.9.6. Medical or mental health evaluations which indicate impairment of the individual's judgment or reliability. The report of evaluation must contain a diagnosis, its effect on the individual's judgment or reliability and prognosis along with any additional instructions or restrictions on the use of the information by appropriate medical authority.

8.2.2.9.7. Summaries of actions by Mental Health Clinics, such as, when individual was enrolled in the program; why the person was enrolled; how the program personnel categorized the individual's situation; a diagnosis and Mental Health authorities recommendations regarding subject's ability to safeguard classified information.

8.2.2.9.8. Reports showing the date of successful completion of a rehabilitation program, progress in a rehabilitation program, or the date termed a rehabilitative failure.

8.2.2.9.9. Summaries or actual report of administrative or disciplinary actions to include records of counseling, letters of reprimand, Article 15, Uniform Code of Military Justice

(UCMJ), or courts-martial orders, bankruptcy petitions, discharge orders, or copies of letters of indebtedness.

8.2.2.9.10. Orders or written notification advising the status and location of individuals placed in retraining, on appellate leave, or rehabilitation or confinement status.

8.2.2.9.11. Reports relating to the withdrawal of access, including special access programs, unescorted entry, or decertification from PRP.

8.2.2.10. Forwards to the CAF within 60 days all SIFs returned from the CAF as incomplete. Requests an extension in writing to the CAF if an incomplete SIF cannot be completed in 60 days. When the SIF was established by the CAF, return the original case file to the CAF.

8.2.2.11. Maintains a suspense copy until the CAF has made the final determination, then destroys the SIF. If the individual had SCI access, destroy six months after accountability of the person ceases or when no longer needed, whichever is longer.

8.2.3. Unit Security Manager:

8.2.3. (8FW) Upon receiving derogatory information, 8 SFS/SFAIP will submit a Continuous Evaluation letter to the subjects SM. The SM will notify the unit commander and provide a written response on whether or not to establish a SIF to 8 SFS/SFAIP within the suspense date on the letter.

8.2.3.1. Implements the personnel security program within the organization and provides support to the servicing security activity or SSO.

8.2.3.1. (8FW) SMs will provide 8 SFS/SFAIP with the applicable letters and forms listed in the Security Manager Handbook for SIF establishment. Upon establishment of a SIF, the SM must provide 8 SFS/SFAIP with a monthly written update.

8.2.4. The CAF:

8.2.4.1. Adjudicates the information contained in the SIF and makes a final security clearance and or SCI access determination.

8.2.4.2. Requests a Special Investigative Inquiry from DSS or a Reimbursable Suitability Investigation from OPM when required in order to make an adjudicative decision.

8.2.4.3. Forwards the notification of eligibility decision to the commander (through the MAJCOM or activity SSO for SCI access) and updates the AMS and DCII with the eligibility determination.

8.2.4.4. Initiates and oversees due process procedures when security clearance eligibility and or access is denied, revoked, or suspended.

8.2.4.5. Returns incomplete SIFs to commanders, through the servicing security activity, with a request for: (1) the required documentation; (2) the commander's recommendation (3) an update on the individual's current situation; and or (4) actions taken, expected, or pending.

8.2.4.6. Establishes SIFs when unfavorable information is provided from other government agencies, court-martial orders, information summary reports from DSS, AFOSI reports of investigation, and notification of special access denial from various access granting authorities. Notifies the commander for further action, when necessary.

8.3. Air Force Office of Special Investigations. AFOSI conducts personnel security investigation leads in overseas areas for DSS. All Air Force commanders must report to AFOSI any alleged criminal activity falling under the security standards criteria. A table of offenses by case category that AFOSI investigates is available in AFI 71- 101, Volume I, *Criminal Investigations.*

8.4. Final Unfavorable Administrative Actions.

8.4.1. The CAF is the designated authority to make personnel security determinations that can result in an unfavorable administrative action. Commanders take actions for removal due to unsuitability IAW 5 CFR 731.201-202, Suitability for Government Employment, at the same time as actions are being taken for denial or revocation of a person's security clearance. The unfavorable administrative action on civilian personnel may not include any reference to security clearance issues until the results of the final security adjudication are available.

8.5. Procedures.

8.5.1. General. The CAF will make a final personnel security determination resulting in an unfavorable clearance action on an Air Force member, civilian employee, contractor (for SCI), or any other Air Force affiliated person when the individual concerned has been afforded due process procedures according to this AFI and DOD 5200.2-R. These same due process procedures are also applicable for suspension, denial, or revocation of access to SCI. There is no distinction between a security clearance and SCI access in the adjudication process. If a clearance is revoked or denied, SCI access is also revoked or denied. The CAF will notify individuals concerning unfavorable administrative actions using the instructions in this AFI and DOD 5200.2-R. Although SAP access is also revoked or denied when a clearance is revoked or denied, administrative recourse (appeal) procedures are separate and distinct. See AFI 16-702, *The Appeal Board (for Special Access Programs).*

8.5.2. The Air Force is not authorized to make any adverse security clearance determination on a civilian employee occupying a nonsensitive position. Since such positions do not involve sensitive duties or access to classified information, the provisions of the personnel security program regarding security clearance eligibility do not apply.

8.5.3. Confinement. When it is determined that an applicant for a security clearance, or a person holding a clearance, has been convicted of a crime and sentenced to imprisonment for more than one year, the clearance of such person shall be denied or revoked with the following actions taken by the CAF:

8.5.3.1. Verification that the individual is presently imprisoned, serving a term of more than 12 months.

8.5.3.2. A Notice of Revocation or Denial of Security Clearance Eligibility forwarded through the Servicing Security Activity and SSO (for SCI) to the individual and the commander. The Notice is final and no rebuttal privileges or appeal rights are applicable.

8.5.3.3. The revocation or denial action is entered in DCII and AMS.

8.6. Unfavorable Administrative Action Procedures.

8.6.1. Denial Authority. The CAF provides individuals with written statements of reasons and other required documentation stating intent to deny or revoke their security clearances and SCI access using sample format in DOD 5200.2-R, App L and Atch 11.

8.6.2. Instructions. Individuals may appeal unfavorable administrative actions according to the instructions in this AFI, DOD 5200.2-R, Chapter 8, and Appendix L and M. Individuals send communications to the CAF and the local supporting Staff Judge Advocate (SJA) through their commanders.

8.6.3. Designated Point of Contact (POC). Unit commanders will designate a POC to serve as a liaison between the CAF and individuals under their jurisdiction when unfavorable administrative actions are being taken. POCs conduct the associated duties as outlined in DOD 5200.2-R, Appendix L-2. The CAF will send communications to the individual through the commander, SF, and SSO (for SCI). The supporting SJA will provide the Defense Office of Hearings and Appeals (DOHA) Administrative Judge (AJ) appropriate legal support, upon request.

8.6.4. Individual's Response to the CAF. Individuals must advise the CAF in writing of their intent to respond to the statements of reasons. This must be done within ten days of receipt of the statement of reasons. Individuals state whether they intend to submit statements or documents to refute, correct, or mitigate the intended actions. Within 60 days from the date of receipt of statements of reasons, individuals must provide the CAF with their written rebuttals.

8.6.5. Extensions. Extensions may only be granted by the CAF. A written request for an extension for up to 30 days can be submitted to the CAF through the POC and installation or unit commander.

8.6.6. CAF Review of Individual's Response to the Statement of Reasons. Upon receipt of the rebuttal, the CAF will determine whether a security clearance should be reinstated, revoked, or denied and a final response will be provided to the individual. This must be done within 60 days from the date of receipt of the individual's response. If a final response cannot be completed within 60 days, the individual must be notified in writing of this fact, the reasons, and the date a final response is expected. AMS will be updated to reflect the CAF decision.

8.6.7. CAF Decision to Deny or Revoke. If the CAF decision is to deny or revoke a person's security clearance the reasons for the final action will be included in a Letter of Denial/Revocation to the individual. Individuals will be afforded an opportunity to appeal to a letter of denial/revocation through the Personnel Security Appeal Board (PSAB) by ***one*** of two methods as outlined in this section and DOD 5200.2-R: (1) appeal *without* a personal appearance; or (2) appeal *with* a personal appearance before an Administrative Judge (AJ) from DOHA. Individuals must elect either (1) or (2); individuals may not do both. The CAF will process appeal cases as outlined in DOD 5200.2-R, Appendix L and Atch 11.

8.6.7.1. Appeal Without a Personal Appearance. Individuals directly notify the PSAB of their intent to appeal without a personal appearance within 10 days of receipt of the letter of denial/revocation. Address requests to: President, Personnel Security Appeal Board, NAIC/IAN, 5113 Leesburg Pike, Falls Church, VA 22041-3230. Individuals send their appeals to the President of the PSAB within 40 days of receipt of the letter of denial/revocation.

8.6.7.2. Appeal With a Personal Appearance. Individuals include the name and telephone number of the supporting SJA when requesting a personal appearance from DOHA (see Atch 13). The POC will provide this information to the individual. DOHA initially contacts the SJA for support with the appeal proceedings. Individuals advise DOHA in writing of their desire for a personal appearance within 10 days of receipt of the letters of denial/revocation. Copies of these advisement's are provided to the following: the POC, the supporting SJA, and the CAF. The SJA will coordinate with the DOHA AJ to assist in providing legal support, upon request and will advise on legal matters to the commander and the POC. The CAF will provide the individual's

case file to DOHA within 10 days upon DOHA's request. A DOHA AJ will hear the individual's case and forward the file, transcripts, any documentation obtained from the individual, and a recommendation to sustain or overturn the letter of denial/revocation to the PSAB. The deadline for this is 30 days after the personal appearance. The AJ provides the CAF with a copy of the recommendation.

8.6.7.2.1. Within CONUS personal appearances will be conducted at the individual's duty station or at a nearby location for duty stations within the lower 48 states. For personnel assigned OCONUS, the appearances will be conducted at: (1) the individual's duty station or a nearby suitable location; or (2) at DOHA facilities located in the metropolitan area of Washington, DC, or Los Angeles, California. The Director, DOHA or designee determines the appearance location. Travel and TDY costs for the individual will be the responsibility of the employing organization.

8.6.8. Personnel Security Appeal Board (PSAB). The PSAB will review the individuals appeal package, along with DOHA recommendation (if applicable) and notify the individual through the CAF of the board's final decision. See Atch 5 for additional guidance on the PSAB.

8.7. Security Clearance Reinstatement. An individual's commander may request reinstatement of their security clearance 12 months after the effective date of revocation or denial or decision of the PSAB, whichever is later. Requests should be sent to the CAF with the commander's recommendation for approval. The commander includes an explanation on how the individual's behavior has improved and the appropriate documentation corresponding to the reason(s) for the denial or revocation. The documentation required depends on the reason(s) involved, such as, evaluation for mental health issues, evaluation for drug or alcohol abuse; or current financial statement(s).

8.8. Special Access Programs. Administrative due process for special access programs is handled separately. See AFI 16-702, *The Appeal Board (for Special Access Programs).*

8.9. Obtaining Permission to Proceed in Courts-Martial, Administrative Dis charges, and Civilian Removal Actions.

8.9.1. Unit commanders contemplating disciplinary or administrative action against military members or civilian employees that could lead to a discharge or removal must first obtain permission to proceed when personnel hold a special access. Do not take action on personnel who now hold or have held access within the periods specified below, to Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI), SCI, research and development (R&D) special access program, AFOSI special access program, or other special access program information until the appropriate special access program office approves. (Exceptions are for investigative and preliminary administrative procedures until the proposed action has been reviewed and approved by the functional activities having overall ownership for the affected information.) Commanders send a written request to the appropriate special access program functional office for permission to proceed with further processing as outlined below. Apply security classification according to message contents. The request must include:

8.9.1.1. The individual's name, SSAN, age, marital status, duty assignment, unit assignment, date of separation and length of service of the member.

8.9.1.2. The name of the official who authorized SCI or other special access. Include inclusive dates that the person was given access and the units involved.

8.9.1.3. The specific reason for the proposed "for cause" action. Include the maximum sentence and type of separation, or discharge, or dismissal allowable.

8.9.1.4. The type of separation, discharge, or dismissal contemplated in administrative cases, and the commander's recommended type of discharge certificate to be issued.

8.9.1.5. The type of court-martial, to include a description of offenses, with an outline of proposed charges and specifications; data as to any restraint; and any unusual circumstances which may affect the trial.

8.9.1.6. Comparable data for civilian employees.

8.9.1.7. Any other information bearing on the proposed action.

8.9.2. For SCI access contact the servicing MAJCOM or FOA Senior Intelligence Officer (SIO) for persons having current SCI access, and persons debriefed within the past three years, where damage assessment is considered *minimal.* Contact the servicing Special Security Office (SSO) to determine if the individual had SCI access. Commanders will continue to forward "Authority to Proceed" requests, where disclosure could result in *serious* damage, to SSO HQ USAF/INSD for AF Director of Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI) approval. Send the request as a Defense Special Security Communications System (DSSCS) message through the SSO to the MAJCOM or FOA SIO and to SSO HQ USAF/INSD. See AFMAN 14-304 for detailed instructions on how to prepare the DSSCS message.

8.9.3. For SIOP-ESI access contact HQ USAF/XO for persons having current SIOP-ESI and other HQ USAF/XO special access programs and persons debriefed within the past 2 years.

8.9.4. For R&D access contact SAF/AQL for persons having current access to R&D special access programs and persons debriefed within the past year.

8.9.5. For persons who have had a duty assignment with AFOSI and have held an AFOSI special access contact HQ AFOSI/IVO. The personnel records will reflect AFOSI employment or assignment. Commanders contact the local AFOSI detachment commander or HQ AFOSI/IVO to determine if the person held an AFOSI special access.

8.9.6. For multiple accesses, commanders must obtain separate authorizations from each appropriate action agency listed above prior to proceeding.

8.9.7. Processing goals at all command levels must comply with the speedy trial requirement and the potentially more restrictive time requirements in civilian removal actions. Normally, the processing time period should be concluded within 15 days; measured from the date of initiation request, to the date of approval; or denial by the OPR. Voluntary separations of airmen, officers, and civilian resignations will not be handled under these procedures unless they are in lieu of adverse action. For voluntary separations that are in lieu of adverse action, do not allow the separation authority to approve the separation until the appropriate action office grants authority to proceed.

8.9.8. If a commander contemplates a general or special court-martial, processing of the case may proceed through preferral of charges and completion of the investigation required by Article 32, UCMJ together with collateral actions required under Article 32. Under no circumstances may the

charges be referred to trial until the appropriate action office grants authority to proceed. Actions required by this paragraph do not apply to summary court-martials.

8.9.9. If a commander contemplates discharging an enlisted member, processing of a "notification" case or a board hearing entitlement may proceed through giving the member notice of the proposed discharge, obtaining the member's response, scheduling necessary appointments, and conducting those appointments. Under no circumstances may the discharge be "approved" by the separation authority until the appropriate action office grants authority to proceed. For board hearing cases, the processing may proceed through initiation of the case, obtaining the member's response, scheduling necessary appointments, and conducting those appointments. Under no circumstances may the convening authority order the board to be convened to hear the case until the appropriate action office grants authority to proceed.

8.9.10. If a commander or staff agency chief contemplates discharging an officer, the show cause authority may not initiate the discharge, issue the show cause memorandum, or otherwise require officers to show cause for retention until the appropriate action office grants authority to proceed.

8.9.11. If a supervisor contemplates removal action against a civilian employee who holds special access, the supervisor must first coordinate with the servicing CPF. The commander of the unit to which the civilian is assigned will then forward a message to the appropriate Air Force OPR. Under no circumstances may a "notice of proposed removal" be issued until the Air Force OPR grants authority to proceed.

8.9.12. Periodic reporting by the unit commanders should advise the parent MAJCOM and decision authority of any changes to the proposed action every 90 days until the action has been completed. If the nature of the case changes significantly (for example, from discharge to court martial or from voluntary to involuntary discharge), the unit commander should notify the decision authority and seek further instruction. Unit commanders should transmit a final report when the adverse action has been completed. In the final report, include date and place of discharge. If a SIF has been established on the individual, the commander will notify the CAF of the discharge, and request closure of the SIF.

8.9.13. Decision authorities submit an annual report of completed cases showing the number of cases considered, number of approvals and disapprovals, and number pending as of the end of the fiscal year to SAF/AAZ, 1720 Air Force Pentagon, Washington DC 20330-1720. For SCI: Quarterly Reporting Requirement (Jan/Apr/Jul/Oct): MAJCOM and FOA SIOs will submit quarterly reports to 497 IG/INSD (SSO), 229 Brookley Ave, Bolling AFB DC 20332-7040. For case management and control purposes include in the reports (1) name, grade, SSAN, organization; (2) reason for action (drug abuse, minor disciplinary infraction, etc); (3) proposed action (type discharge or court martial); (4) date authority to proceed given by SIO; and (5) current disposition (indicate whether case is open or closed). If closed, show type and date of discharge.

Chapter 9

CONTINUING SECURITY RESPONSIBILITIES

9.1. Evaluating Continued Security Clearance.

9.1.1. Commanders and supervisors:

9.1.1.1. Continuously evaluate cleared personnel to ensure they continue to be trustworthy in accordance with the standards in DOD 5200.2-R, Chapter 2.

9.1.1.2. Determine the appropriate steps to take when information or actions occur that bring into question a person's compliance with the adjudication guidelines. See Chapter 8 for unfavorable administrative actions.

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

9.3. Initial Briefings and Refresher Briefings. Commanders, supervisors, and or security managers provide initial and refresher briefings to individuals with security clearance eligibility to ensure they are knowledgeable to execute security responsibilities tailored to the specific job requirements. These briefings will emphasize the individual's responsibility to meet the standards and criteria for a security clearance as stated in DOD 5200.2-R.

9.4. Foreign Travel Briefing. Individuals possessing a security clearance will report to their security manager or supervisor contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities, when:

9.4.1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

9.4.2. Individuals are concerned that they may be the target of exploitation by a foreign entity.

9.5. Termination Briefing. Security Managers execute AF 2587, **Security Termination Statement** according to AFI 31-401.

Chapter 10

SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS

10.1. Responsibilities. The CAF will establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records under its jurisdiction as required by DOD 5200.2-R, Chapter 10.

10.2. Access Restrictions.

10.2.1. The CAF will approve release of completed reports of investigation to appropriate officials for mission essential needs, such as public trust determinations, suitability determinations and appeal decisions. These reports will be safeguarded according to DOD 5200.2-R, Chapter X and not released further without permission from the CAF. HQ AFOSI may request investigations from DSS.

10.2.2. See AFI 33-332, *Air Force Privacy Act Program* and DOD 5400.7-R/AF Supplement AFI 37-131, *Freedom of Information Act Program.*

10.3. Safeguarding Procedures. Officials authorized to receive completed investigation reports ensure the appropriate safeguarding measures are in place in accordance with DOD 5200.2-R, Chapter X.

Chapter 11

PROGRAM MANAGEMENT

11.1. Responsibilities.

11.1.1. Chief, Information Security Division, Air Force Chief of Security Forces (HQ USAF/XOFI), 1340 Air Force Pentagon, Washington DC 20330-1340, develops Air Force personnel security policy.

11.1.2. Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI) is responsible for SCI policy. HQ USAF/XOI has designated:

11.1.2.1. The 497 IG/INS (CAF), 229 Brookley Avenue, Bolling AFB DC 20332-7040, to serve as the single authority to grant, suspend, deny, or revoke personnel security clearance eligibility's and SCI accesses, as well as the determinations of acceptability or non-acceptability for assignment or retention of personnel in sensitive positions.

11.1.2.2. Air Force Intelligence Security (HQ USAF/XOIIS) as the cognizant security authority (CSA) for the development and promulgation of the Air Force SCI security policy.

11.1.2.3. The Personnel Security Appeal Board as the appeal authority for personnel security clearances and SCI access (see Atch 5).

11.1.3. The CAF is the single issuing authority for LAAs. The CAF is also the Office of Primary Responsibility (OPR) for the LAA, PSP, and SK.

11.1.4. ISPMs at MAJCOM and installation levels implement the personnel security program.

11.1.5. Commanders ensure:

11.1.5.1. Security managers are appointed to implement their personnel security programs.

11.1.5.2. Personnel security program oversight is included in self-inspections, unit inspections, program reviews and metrics.

11.1.5.3. Continuing evaluation of personnel with security clearances (see Chapter 9).

Chapter 12

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX

12.1. Access. The CAF is the approval authority for access to the DCII.

12.1.1. Send written requests to the CAF with justification for access and POC as outlined in the DOD 5200.2-R, Chapter 12.

12.1.2. Include security clearance data on the individuals in the request for approval.

12.1.3. With the deployment of SK, DCII read access is authorized for HQ MAJCOM/FOA/DRU, ISPMs, and SSOs.

12.2. Investigative Data. The adjudicative determination on a person may be deleted from the DCII two years after the employment, current affiliation ends, and or security clearance ends.

12.3. Disclosure of Information. See AFI 33-332, *Air Force Privacy Act Program* and AFI 37-131, *Freedom of Information Act Program.*

12.4. Forms Prescribed. AF 2583, Request for Personnel Security Action; AF 2584, Record of Personnel Security Investigation and Clearance; FD 258, FBI Fingerprint Card; and SF 87, U.S. Civil Service Commission Fingerprint Card.

JAMES M. SHAMESS, Brig General, USAF
Director of Security Forces

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-1102, *Safeguarding Single Integrated Operational Plan (SIOP)*

AFI 16-701, *The US Air Force Special Access Programs*

AFI 16-702*, The Appeal Board (for Special Access Programs)*

AFI 31-401, *Information Security Program Management*

AFI 33-332, *Air Force Privacy Act Program*

AFI 34-301, *Nonappropriated Fund Personnel Management and Administration*

AFI 36-2005, *Appointment in Commissioned Grades and Designation and Assignment in Professional Categories Reserve of the Air Force and United States Air Force*

AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*

AFI 41-210, *Patient Administration Functions*

AFI 71-101, Volume I, *Criminal Investigations*

AFH 31-502, *Personnel Security Program Policy*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI)*

AFMAN 37-139, *Records Disposition Schedule*

AFPD 31-5, *Investigations, Clearances, and Program Requirements*

AFPD 34-3*, Nonappropriated Funds Personnel Management and Administration*

DCID 6/4*, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information"*

DODM 4525-8AFSUP1*, Official Mail Manual.*

DOD S-51105.21-M-1, *Sensitive Compartmented Information Administrative Manual*

DOD Regulation 5200.2-R, *DoD Personnel Security Program*

DOD 5210.42, *Nuclear Weapons Personnel Reliability Program*

DOD 5210.55, *Department of Defense Presidential Support Program*

DOD 5210.87, *Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities*

DOD 5400.7-R/AF Supplement 37-131*, Freedom of Information Act Program*

Abbreviations and Acronyms

AF—Air Force

AFH—Air Force Handbook

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFR—Air Force Regulation

AFSC—Air Force Specialty Codes

AIS—Automated Information Systems

AMS—Adjudication Management System

ANACI—Access National Agency Check with Written Inquiries and Credit Check

ASCAS—Automated Security Clearance Approval System

BI—Background Investigation

CAF—Central Adjudication Facility

CAVS—Clearance and Access Verification System

CEIC—Catch'Em In CONUS

CONUS—Continental United States

CPF—Civilian Personnel Flight

DCII—Defense Clearance and Investigations Index

DCID—Director of Central Intelligence Directive

DCPDS—Defense Civilian Personnel Data System

DSS—Defense Security Service

DOD—Department of Defense

DRU—Direct Reporting Unit

ENTNAC—Entrance National Agency Check

EPSQ—Electronic Personnel Security Questionnaire

ESI—Extremely Sensitive Information

FBI—Federal Bureau of Investigations

FOA—Field Operating Agency

HQ USAF—Headquarters United States Air Force

IMA—Individual Mobilization Augmentee

ISPM—Information Security Program Manager

LAA—Limited Access Authorization

LFC—Local Files Check

MAJCOM—Major Command

MEPS—Military Entrance Processing Station

NAC—National Agency Check

NACIC—National Agency Check with Written Inquiries and Credit Check

NACLC—National Agency Check with Local Agency Check and Credit Check

NAFI—Nonappropriated Fund Instrumentalities

NAQ—National Agency Questionnaire

NATO—North Atlantic Treaty Organization

NdA—Nondisclosure Agreement

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

PCS—Permanent Change of Station

PCIII—Personnel Concept III

PDS—Personnel Data System

PR—Periodic Reinvestigation

PRP—Personnel Reliability Program

PSAB—Personnel Security Appeal Board

PSI—Personnel Security Investigation

PSO—Program Security Officer

PSP—Presidential Support Program

PSQ—Personnel Security Questionnaire

R&D—Research & Development

SAC—Single Agency Check

SAF—Secretary of the Air Force

SAP—Special Access Program

SAR—Security Access Requirement

SBI—Special Background Investigation

SCI—Sensitive Compartmented Information

SIF—Security Information File

SII—Special Investigative Inquiry

SIOP—Single Integrated Operational Plan

SIOP-ESI—Single Integrated Operational Plan -Extremely Sensitive Information

SK—SENTINEL KEY

SSN—Social Security Number

SSBI—Single Scope Background Investigation

SIF—Security Information File

TDY—Temporary Duty

UCMJ—Uniform Code of Military Justice

UIF—Unfavorable Information File

UMD—Unit Manpower Document

U.S.C.—United States Code

497 IG/INS—497th Intelligence Group/Directorate of Security and Communications Management

Terms

Authorized Requester—Organizations authorized to request Personnel Security Investigations (PSIs) from DSS or OPM. The servicing security forces activity usually requests PSIs from DSS. The CPF requests National Agency Check with Written Inquiries and Credit Check (NACICs) and Access National Agency Check with Written Inquiries and Credit Check (ANACIs) from OPM.

Authorized Requester Code Listing—A listing of organizations specifically designated by MAJCOM, FOA, or DRU to request PSIs.

Break In Service—Any break in active employment with a Federal agency or DOD contractor, including suspension or termination of service or temporary retirement, whether or not seniority or pay is affected. This does not include active duty military personnel attending civilian schools from which a service commitment remains. A 24-month continuous break in service requires completion of a new PSI prior to reissuance of a security clearance eligibility.

Catch'Em In CONUS—A DSS Program utilized to facilitate the completion of an SSBI or SSBI-PR on individuals who are within 180 days of departing for an overseas assignment. This program allows the DSS investigator to conduct the personal interview prior to PCS.

Central Adjudication Facility (CAF)—A single facility designated by the head of the DOD Component to evaluate PSIs and other relevant information and to render final personnel security determinations. The 497 IG/INS is the CAF for the Air Force.

Classified Information Nondisclosure Agreement, Standard Form 312—An individual must sign a Standard Form 312 before being given access to classified information.

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

Continuing Evaluation—Procedures employed to ensure an individual remains eligible for access to classified information.

Critical Sensitive Position—Include positions involving any of the following: Access to Top Secret defense information; development or approval of war plans, plans or particulars of future or major special operations of war, or critical and extremely important items of war; investigative duties, the issuance of personnel security clearances, or duty on personnel security appeal boards, computer and or computer-related positions designed AIS I, or other positions related to national security, regardless of duties that require the same degree of trust.

Defense Civilian Personnel Data System (DCPDS)—Method used to transmit civilian personnel data to or from an installation.

Defense Security Service (DSS)—The personnel security investigative agency for DOD to include the military departments, defense agencies and DOD contractors.

Escorted Entry—A situation where personnel are required to be escorted into a restricted area and kept under surveillance by authorized personnel while in the area.

Foreign National—Any person who is neither a citizen nor national of the United States nor an immigrant alien. Also referred to as a non-United States national.

Foreign Travel—Any travel outside the 50 United States and its territories.

Immediate Family—Includes: father, mother, brother, sister, spouse, cohabitant, son, daughter. The basis of the relationship is immaterial: included are stepparents, foster parents, brothers and sisters by adoption, half-brothers and half-sisters, foster brothers and sisters, adopted children, stepchildren, and foster children.

Indoctrination Briefing—A briefing of job related security responsibilities and requirements, intelligence collection techniques employed by foreign intelligence activities, and penalties that may be imposed for security violations.

Installation Records Check—An investigation conducted through the records of all installations of an individual's identified residences for the preceding 2 years before the date of the application. This record check shall include at a minimum, police (base and or military police, security office, or criminal investigators or local law enforcement) local files check, Drug and Alcohol Program, Family Housing, Medical Treatment Facility for Family Advocacy Program to include Service Central Registry records and mental health records, and any other record checks as appropriate, to the extent permitted by law.

Local Files Check (LFC)—A local check of the security forces, medical facility, personnel files, etc., designed to uncover the existence of unfavorable information concerning a person.

Nonappropriated Fund Instrumentalities (NAFI) Employee—Personnel hired by the DOD components, compensated from NAFI funds. This includes temporary employees, 18 years or older, who work with children.

Nonappropriated Fund Position of Trust (NAF)—An employee whose duties are fiduciary in nature and require a high degree of trust and integrity to ensure the safety of people, protection of money or property or who could directly and adversely affect the mission of the organization.

Noncritical-Sensitive Position—Includes positions that involve access to Secret or Confidential national security material or information; or duties that may directly or indirectly adversely affect the national security operations of the agency.

Personnel Data System (PDS)—Method used to transmit personnel data from or to an installation.

Personnel Reliability Program (PRP)—A program designed to ensure the highest possible standards of individual reliability in personnel performing duties associated with nuclear weapons systems and critical components.

Personnel Security—A criterion of security based upon standards that must be met for clearance or assignment to sensitive duties. The allegiance, reliability, trustworthiness and judgment of the individual being considered for such positions must be assessed to ensure that the placement of each individual in

such a position is clearly consistent with the interests of national security.

Personnel Security Appeal Board—Designated representatives review appeals to denials or revocations of security clearances.

Presidential Support—Personnel assigned to duties involving regular or frequent contact with or access to the President or Presidential facilities, communication activities, or modes of transportation.

Program Security Officer—The government official who administers the security policies for the Special Access Program (SAP).

Restricted Area—A legally established military zone under Air Force jurisdiction into which persons may not enter without specific authorization.

Secret Clearance—The individual has been granted eligibility to information classified Secret or below.

Security Access Requirement—A code used to manage and control security clearances within the Air Force. It identifies the level of access required for day-to-day job performance. The security access requirement code is based upon the supervisors or commanders determination of level of access required for each position and the security clearance eligibility determined by the CAF for the incumbent.

Security Clearance—A determination that a person has met the standards of DOD and Air Force personnel security programs for eligibility to classified information.

Sensitive Compartmented Information (SCI)—Classified information concerning or derived from intelligence sources, methods, or analytical processes which must be processed exclusively within formal access control systems established by the Director of Central Intelligence.

SENTINEL KEY—The Air Force system of records for personnel security and access information. Replaces the ASCAS.

Service—Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in government service, or civilian employment with a DOD contractor involving access under the National Industrial Security Program. Continuity of service is maintained with change from one status to another provided no single break in service is greater than 24 months.

SCI Screening Interview—A representative from the SSO or a security manager will conduct an interview to assist in determining the acceptability of an individual for nomination and further processing for a position requiring access to SCI. This interview is conducted when there is no current investigative information available to make an adjudicative determination of eligibility for immediate access to SCI.

Sensitive Position—Any civilian position designated within the Air Force wherein the occupant could cause by virtue of the nature of the position a materially adverse effect on national security. All federal civilian positions are designated either special sensitive, critical sensitive, noncritical sensitive, or nonsensitive.

Servicing Security Activity—The activity, designated by the commander, that supports the installation population and tenant units in all areas of personnel security program implementation.

Single Agency Check—A check of one or more designated agencies of a NAC.

Single Scope Background Investigation (SSBI)—A PSI covering 7 years of a person's history (10 years for employment, residence, and education). It is used to determine acceptability for a Top Secret security

clearance, access to specific special access programs, or access to SCI.

Top Secret Clearance—The individual has been granted eligibility to Top Secret information or below.

Trustworthiness Determination—A determination made by commanders to protect DOD property and resources under their jurisdiction.

Unescorted Entry—Authority for an individual to enter and move about a restricted area without escort.

Unfavorable Information—Information that could justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

Unfavorable Personnel Security Determinations—A denial or revocation of a person's security clearance; denial or revocation of access to classified information; denial or revocation of special access authorization (including SCI access); non-appointment to or non-selection for appointment to a sensitive position; non-appointment to or non-selection for any other position requiring a trustworthiness determination; reassignment to a position of lesser sensitivity or to a nonsensitive position; and non-acceptance for or discharge from the armed forces when any of the foregoing actions are based on derogatory information of personnel security significant.

Attachment 1 (8FW)

GLOSSARY OF REFERENCES, ABBREVIATIONS AND ACRONYMS

References

AFI 31-401, *Information Security Program Management*

DOD 5200.2, *DOD Personnel Security Program*

AF Form 2583, *Request for Personnel Security Action*

SF Form 312, *Classified Information Nondisclosure Agreement*

Abbreviations

CAVS—Clearance and Access Verification System

EPSQ—Electronic Personnel Security Questionnaire

JPAS—Joint Personnel Adjudication System

NDA—Non- disclosure Agreement

PSI—Personnel Security Investigations

SAR—Security Access Requirement

SIF—Security Information File

SM—Security Managers

Attachment 2

REQUEST PROCEDURES

A2.1. General.

A2.1.1. Security managers:

A2.1.1.1. Process completed personnel security questionnaires for active duty, reserve military, National Guard, civilian and or contractor personnel to the unit's supporting authorized requester of investigations IAW with this AFI. See Atch 3 for required security forms, types of investigations to request and in what situations. An individual must have one year retainability before an investigation may be requested.

A2.1.1.2. Verify the most recent or most significant claimed attendance, degree or diploma at an educational institution.

A2.1.1.3. Verify the date and place of birth through a check of appropriate documentation, e.g., a birth certificate, certificate of naturalization, passport, or Report of Birth Abroad of a Citizen of the United States of America.

A2.1.1.4. Show the verification of birth and highest level of education on the EPSQ.

A2.1.2. The subject will provide the required documentation to the security manager. In rare circumstances when the subject is unable to provide the documentation, the subject will prepare a written declaration verifying the date and place of birth and education attendance. The statement will be kept with the security manager until the subject receives a security clearance.

A2.1.3. Air Force Reserves and IMAs. The Air Force Reserve Recruiting Service (AFRC/RS) processes reservist's initial personnel security investigation during accession to the supporting authorized requester. When Electronic Personnel Security Questionnaire (EPSQ) capability is not available for the subject to enter the data, the AFRC/RS may submit paper copy of SF 86 to the supporting authorized requester. Exception to this process would be those applicants which are required to have a Top Secret security clearance prior to entering or completing technical school (as required in AFCAT 36-2223, USAF Formal Schools). In this case, the reserve recruiter will provide a completed electronic version of EPSQ to the supporting unit security manager, active duty security manager or authorized requester.

A2.2. Authorized Requesters.

A2.2.1. Authorized Requesters:

A2.2.1.1. Request personnel security questionnaires. See Atch 3, for required security forms and or software, types of investigations to request and in what situations. Request investigations from DSS or OPM.

A2.2.1.2. Use the EPSQ software as the primary source for the investigative request.

A2.2.1.3. Electronically transmit the validated questionnaire to DSS. See AFI 36-2104, *Nuclear Weapons Personnel Reliability Program,* for processing PSI questionnaires on PRP candidates and certified personnel.

A2.2.1.3.1. Attach the prepared file to an Internet email. Check DSS web site for the latest email address. No information is necessary in the body of the email.

A2.2.1.3.2. DSS posts receipts for all electronically transmitted requests and mailed diskettes in the DSS EPSQ Receipt System on the DSS web site.

A2.2.1.3.3. For additional EPSQ guidance contact the DSS web site. Contact DSS Customer Service Center at 1-800-542-0237 or DSN 283-7731, if necessary.

A2.2.1.3.4. In cases where electronic transmission is not possible, use the EPSQ software and mail the diskette to DSS according to the instructions in Atch 22.

A2.2.1.4. Use the EPSQ software at the unit, validate the EPSQ, and print a hard copy for mailing investigation requests to OPM. OPM does not have electronic transmission capability. OPM address: OPM-FIPC, PO Box 618, 1137 Branchton Road, Boyers, PA, 16018.

A2.2.1.5. Maintain a suspense copy of PSIs and all other information until the investigative data appears in the CAVS.

A2.2.1.6. Forward the original signed "Authorization for Release of Information," and if applicable, the "Authorization for Release of Medical Information" to DSS/Operations Center-Baltimore (OCB), P.O. Box 28989, Baltimore, Maryland 21240-8989 or to OPM.

A2.2.1.7. Forward the suspense copy of the PSI to the gaining base authorized requester when a permanent change of station (PCS) occurs.

A2.3. IMAs. The authorized requester of the unit of assignment or attachment will submit periodic reinvestigations or confirm revalidation's of security clearances for IMAs.

A2.4. Catch'Em in Continental United States (CONUS) (CEIC) Program. Personnel requiring an SSBI or periodic reinvestigation and who are scheduled for a PCS move to an overseas location, including Shemya AFB, AK, fall within the CEIC program. Such individuals must complete the personnel security questionnaire within 180 days prior to departure. This allows the DSS investigator to conduct the personal interview before they PCS.

A2.5. Subject Interview. Individuals completing a personnel security questionnaire must specify any circumstances that would make them unavailable for a subject interview within 180 calendar days of the date the form is transmitted. Detailed information regarding the period in which the individual will be unavailable such as date, location, and duration should be provided in the remarks section of the appropriate form. DSS or OPM will try to conduct the subject interview prior to departure of the individual.

A2.6. Local Files Check. The unit security manager initiates and verifies completion of a LFC that includes a review of local personnel, medical facility, law enforcement, or other security records, as appropriate. Use AF Form 2583, **Request for Personnel Security Action**, to document an LFC. See Atch 23 for instructions on filling out AF Form 2583.

A2.6.1. Headquarters Air Education and Training Command/Recruiting Service (HQ AETC/RS), 550 D Street West, Suite 1, Randolph AFB TX 78150-4527 does not have to complete AF Form 2583 when personnel records are unavailable.

A2.6.2. The Reserve Recruiting Service (HQ AFRC/RS) or their authorized requesters do not have to complete AF Form 2583 for IMAs, IRRs, and traditional reservists when personnel records are unavailable.

A2.6.3. AF Form 2583 is not needed for civilian applicants for federal employment when local files are unavailable.

A2.6.4. Record briefings for access to special access program information on AF Form 2583 when the governing program directive does not prescribe other procedures.

A2.7. National Agency Check. Authorized requesters submit an SF 85P and an SF 87 to OPM-FIPC, PO Box 618, 1137 Branchton Road, Boyers, PA, 16018. Investigations that contain overseas leads should be transmitted via EPSQ to DSS. Use the EPSQ software at the unit and print a hard copy for mailing.

A2.8. National Agency Check with Written Inquiries and Credit Check. The CPF will submit an original and one copy of SF 85 or SF 85P, as appropriate to OPM. Include an SF 87 and mail directly to the: US Office of Personnel Management - FIPC, PO Box 618, 1137 Branchton Road, Boyers, PA, 16018.

A2.9. Access National Agency Check with Written Inquiries and Credit Check. For civilians requiring access to classified information at the Secret level in order to perform mission duties or in non-critical sensitive positions, the CPF will submit an original and one copy of SF 86 and an SF 87 to OPM-FIPC PO Box 618, 1137 Branchton Road, Boyers, PA, 16018. Use the EPSQ software at the unit and print a hard copy for mailing.

A2.10. National Agency Check with Local Agency Checks and Credit Check. Authorized requesters transmit an SF 86 via EPSQ to DSS for individuals requiring access to SECRET information. Mail a signed original of FD258 to DSS. DSS address: DSS, PO Box 28989, Baltimore, MD, 21240-8989.

A2.10.1. This includes all SECRET level SAPs.

A2.10.2. The SF 86 must cover the most recent seven-year period. The "Have you ever" questions cover the individuals entire lifetime.

A2.10.3. NACLCs will be requested for individuals with no prior or current security clearance eligibility if and when access to Secret information is required regardless of the age of an existing investigation.

A2.10.4. Existing ENTNAC or NAC investigations remain valid for individuals with prior or current SECRET eligibility regardless of the age of the investigations if there has been no break in service over 24 months. Periodic reinvestigation rules apply.

A2.11. Single Scope Background Investigation. Authorized requesters transmit DD Form 1879 and an SF 86 via EPSQ to DSS for military, guard, reserve, or contractor personnel. DSS should receive requests for civilian personnel investigations that contain overseas leads (subject currently resides overseas or has resided overseas during the scope of the investigation). For investigations that don't contain overseas leads, use EPSQ software, validate the EPSQ, and print a hard copy of the EPSQ to mail to OPM for civilian personnel. Mail a signed copy of the "Authorization for Release of Information" with the original of FD 258 to DSS or the original of SF 87 to OPM. DSS address: DSS, PO Box 28989, Baltimore, MD,

21240-8989. OPM address: OPM-FIPC, PO Box 618, 1137 Branchton Road, Boyers, PA, 16018.

A2.11.1. The questionnaire must be completed to cover the most recent seven-year period with 10 years coverage on the residence, education, and employment questions, or since the 18th birthday, but at least the last two years. "Have you ever" questions must cover the individuals entire lifetime. For those authorized to submit hard copy, use SF 86A, **Continuation Sheet for Questionnaires** for information for years 8 through 10. The EPSQ (Version 2.0) will accept 10 years of data.

A2.11.2. A Single Agency Check is required on the following individuals associated with the subject of an SSBI: (a) spouse or cohabitant, (b) immediate family members 18 years old or older who were born outside the United States. If marriage or cohabitation occurs after completion of the SSBI, transmit Spouse SAC via EPSQ to DSS. Keep a hard copy for authorized requester's suspense file.

A2.11.3. Provide both the alien and naturalization/citizenship number for each foreign-born relative and associate listed on the SF 86 that claims US citizenship. Other authorized means in proving U.S. citizenship for foreign-born relatives are the State Department form 240, Report of Birth Abroad of a citizen of the U.S., or the number from either a current or previous U.S. passport.

A2.11.4. If selective service number is not known, the subject's SSAN will be accepted.

A2.12. Periodic Reinvestigation.

A2.12.1. Transmit DD Form 1879 and SF 86 via EPSQ to DSS for military, guard, reserve or contractor personnel. DSS should receive requests for civilian personnel investigations that contain overseas leads (subject currently reside overseas or has resided overseas during the scope of the investigation). For investigations that don't contain overseas leads, use EPSQ software, validate the EPSQ, and print a hard copy of the EPSQ to mail to OPM for civilian personnel. No abbreviated version of SF 86 or EPSQ may be submitted in connection with a PR. A person must have one-year retainability before a periodic investigation may be requested.

A2.12.2. An authorized requester should initiate a SECRET Periodic Reinvestigation (S/PR) 10 years from the date of the previous investigation or reinvestigation. Questionnaire must cover the most recent 10-year period or the period since the last investigation.

A2.12.2.1. Applies to reinvestigations for access to Secret (including Secret SAP) or noncritical sensitive positions.

A2.12.3. An authorized requester should initiate a TOP SECRET Periodic Reinvestigation (SSBI-PR) 5 years from the date of the previous investigation or reinvestigation.

A2.12.3.1. Applies to reinvestigations for access to TOP SECRET (including TOP SECRET SAPs), SCI, and eligibility for occupancy of a critical sensitive position.

A2.12.3.2. If the date of the last investigation is between five and seven years old, the SSBI-PR will cover the entire period of time.

A2.12.3.3. If the date of the last investigation is between eight and ten years old, the SSBI-PR will only cover the last seven years except for local agency checks which will cover up to ten years.

A2.12.3.4. If the date of the last investigation is more than ten years old, the SSBI-PR will only cover the last seven years except for local agency checks which will cover up to ten years.

A2.12.3.5. In all SSBI-PRs, the subject interview need not be constrained by time nor will any SSBI-PR that reveals adverse information. All such cases will be fully expanded in accordance with the national investigative policy.

A2.12.4. For individuals in a NATO billet, submit the PR 48 months from the date of the previous investigation or reinvestigation.

A2.13. Air Force Liaison Office at the Operations Center-Baltimore. Call the AFLNO for cancellations, responses to queries from the AFLNO, or with permission from the CAF. Address for the AFLNO is: Defense Security Service, ATTN: Air Force Liaison Office, PO Box 46060, Baltimore, MD, 21240-6060.

A2.14. Overnight Mail. Address for sending overnight mail to the AFLNO is: Defense Security Service, ATTN: Air Force Liaison Office, 881 Elkridge Landing Road, Linthicum, MD, 21090.

Attachment 3

TABLES FOR INVESTIGATIONS AND ASSIGNING SECURITY ACCESS REQUIREMENTS (SAR)

A3.1. Security Investigations, Forms, and EPSQ. Use the following table for guidance on the types of required security investigations and appropriate forms and or Electronic Personnel Security Questionnaire (EPSQ).

Table A3.1. Security Investigations, Forms, and EPSQ.

RULE	A Type of Investigation	B DD Form 1879	D EPSQ (see note 1) or SF 86/85P/85	E FD Form 258 or SF 87 (see note 3)
1	NAC		SF 85P	1 signed original of SF 87 (mail with packet to OPM)
2	NACLC including Secret/PRs and SAP/ PRs		SF 86 (see note 2)	1 signed original of FD Form 258 (except PRs)
3	NACIC		Original and 1 copy of SF 85/85P	1 signed original of SF 87 (mail with packet to OPM)
4	ANACI		Original and 1 copy of SF 86	
5	SSBI including TS/PRs		SF 86 (see notes 2 & 4)	1 signed original of FD Form 258 (except civilians)
6	Special Investigative Inquiry	Original and 1 copy.	Original and 2 copies of SF 86 (see notes 5 & 6)	1 signed original if FBI/ID check desired

NOTES:

1. Use electronic transmission to DSS and keep original signature suspense copy until investigative data is reflected on SK. If electronic capability does not exist, use EPSQ software and mail validated request on a disk to DSS (see Atch 22 for instructions). When authorized by HQ USAF/XOFI, use EPSQ software, print hard copy, and mail to DSS.

2. Civilian SSBI and PR investigations will be submitted to OPM until otherwise notified. Investigations with overseas leads will be submitted to DSS. Use the EPSQ at the unit and print the SF 86 for mailing along with the signed releases and SF 87.

3. Mail Signed Releases and Fingerprint Cards to DSS or OPM.

4. If marriage or cohabitation occurs after completion of the SSBI, submit Spouse SAC via EPSQ to DSS. Keep one copy for authorized requester's suspense file.

5. Send original and 1 copy to the CAF for forwarding to DSS. One copy is for the authorized requester's suspense file.

6. An original copy of the SF 86 (or EPSQ) should accompany the request, where appropriate, unless such documentation was submitted within the last 12 months to DSS or OPM as part of another PSI. The results of any other recently completed investigative reports should also be sent. Indicate the specific areas or issues requiring investigation with justification in Remarks.

A3.2. Requesting NAC/NACIC Investigations. Use the following table for guidance on NAC and NACIC investigations as a minimum requirement for positions having no access to classified information.

Table A3.2. Requesting NAC/NACIC Investigations.

RULE	A **If the individual is a**	B **and duties require**	C **Then a NAC/NACIC is required**
1	Person requiring unescorted entry (see note 1)	**unescorted entry into restricted areas, access to sensitive areas, or equipment**	NAC for military & contractor employee NACIC for DOD civilian Before entry or access (see notes 2 & 3)
2	Nonappropriated fund employee	employment in a position of trust	NAC before performing duties (see note 4)
3	Person requiring a DOD building pass	a DOD building pass	NAC before issuance
4	Foreign national employed overseas	no access to classified information	NAC before employment (see note 5)
5	Person requiring access to chemical agents	access to or security of chemical agents	NAC before assignment
6	Civilian nominee for military education and orientation program	education and orientation of military personnel	A NACIC before performing duties (process limited access authorization for non-United States citizens) (foreign educators are employed in non-critical sensitive positions)
7	Contract guard	performing guard functions	NAC prior to assignment
8	Person assigned to AIS II or III positions	Assignment to AIS II or III (formerly ADP) positions	NAC for military & contractor employee NACIC for DOD civilians

NOTES:

1. A NACLC is a prerequisite for military members upon entry. DOD civilians receive a NACIC as a prerequisite for federal employment. These investigations exceed the required investigations and can be used for unescorted entry.

2. Air Reserve forces personnel with a current ENTNAC or NAC on file may have unescorted entry to restricted areas while in civilian status, pending completion of the required NACIC.

3. Prior ENTNAC/NAC/NACI/NACIC investigations meet the requirements for prior military members who have been separated. Commanders may waive on a case by case basis, the investigative requirements for unescorted entry to restricted areas containing Protection Level (PL) 2 and or 3 resources pending completion of a favorable NACLC, NAC, or NACIC after favorable review of the completed personnel security questionnaire for the investigation.

4. Installation records checks on employees in child care services include a check of the state criminal history repository. The state criminal history repository checks are for suitability affecting the consolidated civilian personnel office and morale, welfare, and recreation programs. The sponsoring activity sends out and receives the state criminal history repository.

5. The NAC must consist of: (a) host-government law enforcement and security agency records check at the city, state, province, and national level, (b) DCII check, and (c) FBI check where information exists indicating residence by the foreign national in the United States for one year or more since the age 18.

A3.3. Requesting NACLC/ANACI Investigations. Use the following table for guidance on NACLC and ANACI investigations required for access to classified information.

Table A3.3. Requesting NACLC/ANACI Investigations.

RULE	A If the individual is a	B and duties require	C Then a NACLC/ANACI is required
1	United States military member	a Secret clearance	NACLC before granting final clearance
2	Prior military member reentering Air Force after a break in military service exceeding 24 months	retention in the Air Force to include Air Reserve forces	NACLC to be initiated no later than 3 work-days after reentry
3	Applicant for appointment as a commissioned officer	Commissioning as an officer, includes Air Reserve forces	NACLC before appointment (after appointment for health professionals, chaplains, and attorneys) (see note 1)
4	Air Force academy cadet, military academy cadet, or naval academy midshipman	Enrollment	NACLC to be initiated 90 days after entry
5	Reserve officer training candidate or midshipman	entry to advanced course of college scholarship program (see note 2)	NACLC to be initiated 90 days after entry
6	United States military member	customs inspector duty	NACLC before assignment
7	DOD military or contract employee	access to or security of chemical agents	NACLC before assignment
8	United States military member, civilian, or contract employee	assignment to North Atlantic Treaty Organization positions	NACLC for military and contractor employee, ANACI for civilian employee
9		secret special access programs	Before performing duties and at 5-year intervals thereafter while assigned
10		assignment to Category III PSP	
11		assignment to a controlled PRP position	NACLC for military and contractor employee, ANACI for civilian employee before PRP certification

NOTES:

1. The individual must agree in writing that if the results of the investigation are unfavorable, the individual will be subject to discharge. Under the exception, commissions in the reserve components other than the National Guard may be offered to immigrant alien health professionals, chaplains, and attorneys.

2. Reserve officer training candidate graduates who delay entry on active duty pending completion of further college study are not authorized a new NACLC once they have been commissioned. Request recertification when the officer comes on active duty.

A3.4. Guide for Requesting SSBIs. Use the following table for guidance on the minimum standards required for SSBIs.

Table A3.4. Guide for Requesting SSBIs.

RULE	A If the individual is a (an)	B and duties require	C then a favorably completed SSBI is required before
1	United States military member, civilian, or contractor employee	Top Secret clearance	granting final clearance
2		assignment to a "critical or special sensitive position"	assignment to position
3		assignment to a "critical" position in the personnel reliability program	PRP certification
4		AIS I (formerly ADP I) positions	assignment
5		assignment to a category I or II presidential support position	within 36 months prior to selection
6		access to North Atlantic Treaty Organization COSMIC Top Secret or COSMIC Top Secret ATOMAL	access may be granted
7		access to SCI or an approved special access program	granting access
8		access to SIOP-ESI	
9		Assignment to the National Security Agency	Assignment
10		Assignment to the Defense Courier Service	
11		Assignment to personnel security adjudicative functions, counterintelligence, or criminal investigative or direct investigative support duties	
12	immigrant alien	limited access to Secret or Confidential information	issuing limited access authorization
13	non-United States national employee		
14		the education and orientation of military personnel	performing duties
15		Unescorted entry to PL 1 and 2 restricted areas	authorized entry

A3.5. Guide For Requesting Periodic Reinvestigations. Use the following table for guidance on the minimum standards for Periodic Reinvestigations.

Table A3.5. Guide For Requesting Periodic Reinvestigations.

R	A	B	C
U L E	If the individual is a	and duties require	then request a periodic reinvestigation
1	United States military member, DOD civilian, or contractor employee	access to Top Secret	5 years from the date of the last SSBI or SSBI-PR
2		access to SCI	
3		assignment to presidential support	
4		assignment to an AIS I position	
5		access to SIOP-ESI	
6		assignment to AFOSI duties	
7		assignment to a critical personnel reliability program position	
8		access to Top Secret special access programs	
9	United States civilian employee	assignment to a special or critical sensitive position	
10	Non-United States national employee and immigrant alien	limited access authorization	
11		unescorted entry to PL 1 or 2 restricted areas	
12	United States military member, DOD civilian, or contractor employee	North Atlantic Treaty Organization COSMIC Top Secret or COSMIC Top Secret ATOMAL	54 months from the date of the last SSBI or SSBI/PR
13	United States military member, DOD civilian, or contractor employee	access to an approved Secret special access program	54 months from the date of the last investigation
14		Explosives Ordinance Disposal	
15		assigned to a North Atlantic Treaty Organization staff position	54 months from the date of the last investigation
16		access to Secret information and/or assignment to noncritical sensitive positions	10 years from the date of the last investigation

A3.6. Guide for Requesting Investigations for Unescorted Entry to Restricted Areas. Use the following table for guidance for investigations required for the minimum investigative standards for unescorted entry to restricted areas.

Table A3.6. Guide for requesting investigations for Unescorted Entry to Restricted Areas.

RULE	A	B	C
	If the individual is a (an)	and duties require	Then the following favorably completed Investigation is required before entry
1	U.S. active duty military (includes immigrant aliens)	Unescorted entry into restricted areas, access to sensitive information areas, or equipment	NACLC
2	U.S. retired or separated military member with an Honorable Discharge and no break in service greater than 24 months.		NAC
3	DOD Civilian with no break in federal service greater than 24 months		NACIC (see note 1)
4	NAF employee		NAC
5	DOE employees with no break in service greater than 24 months		NACIC is equivalent to the Department of Energy "L" investigation
6	Federal employees		NAC or equivalent investigation certified by the non DOD agency
7	Contractor employees		NAC
8	Foreign nationals, Other non-US national		SSBI for PL 1 or 2 resources. Local Agency Check for PL 3.
9	Foreign National Military members and host nation military members assigned to USAF activities		Security assurance of favorable investigation based on government-to-government agreements, treaties, (NATO) agreements, for PL 1 & 2. For PL 3, verification of security clearance by foreign commander and authenticated by Security forces or designated representative; personnel foreign travel orders; and the restricted area badge or home-station equivalent controlled picture identification credential.
10	Foreign National Employees Overseas Employed by DOD organizations		Host government law enforcement and security agency checks at the city, state (province) and national level whenever permissible by the law of the host government, DCII, and FBI-HQ/ID (where information exists regarding residence in US for one year or more since age 18).

NOTES:

1. Verification of NACIC can be made by contacting the CPF.

A3.7. Guide For Assigning Security Access Requirement (SAR) Code To Each Authorized Manpower Position. Use the following table for guidance on assigning security access code to each authorized manpower position.

Table A3.7. Guide For Assigning Security Access Requirement (SAR) Code To Each Authorized Manpower Position.

RULE	A If duties require access to	B then security access requirement code is
1	no access required	0 or Blank
2	Secret	1
3	Top Secret	2
4	SIOP-ESI, AFOSI, DOD courier, or Presidential Support	3
5	SCI	S
6	Child Care	4

Attachment 4

DOD SECURITY CLEARANCE AND OR SCI ACCESS DETERMINATION AUTHORITIES

A4.1. Officials Authorized to Grant, Deny, or Revoke Personnel Security Clear ances (Top Secret, Secret). The 497th Intelligence Group/INS, Directorate of Security and Communications Management, the Air Force Central Adjudication Facility, is the designated authority to grant, suspend, deny, or revoke personnel security clearances and SCI access.

A4.2. Officials Authorized to Grant, Deny, or Revoke LAA. The CAF is the single authority to grant, deny, or revoke an individual's LAA.

A4.3. Officials Authorized to Certify Personnel Under Their Jurisdiction for Access to Critical Nuclear Weapon Design Information. Commanders and staff agency chiefs have the authority to grant CNWDI access. This authority is assigned to division chiefs and above at all levels of command. (Refer to AFI 31-401, *Information Security Program Management*).

A4.4. Official Authorized to Approve Personnel for Assignment to Presidential Support Activities. Commanders nominate individuals to the CAF for assignment to Presidential Support Activities. The CAF makes the final recommendation to the DOD Executive Secretary to the Secretary of Defense.

A4.5. Officials Authorized to Grant Access to SIOP-ESI. The Air Force has approved the Chief of Staff, Vice Chief of Staff, Assistant Vice Chief of Staff, and Deputy Chiefs of Staff for SIOP-ESI access and has designated them as SIOP-ESI access granting authorities. These officials may further delegate their access granting authority. (Refer to AFI 10-1102, *Safeguarding the Single Integrated Operational Plan*).

A4.6. Authority to Render Final Appeal Decisions. The Personnel Security Appeal Board is designated as the appeal authority for personnel security clearances and SCI access.

A4.7. Officials Authorized to Suspend Access to Classified Information.

A4.7.1. Security Clearances. Commanders have the authority to suspend access to classified information.

A4.7.2. SCI. Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI) and Senior Intelligence Officers or their designees are the authorities to suspend access to SCI.

A4.8. Official's Authorized to Grant, Deny, Suspend, Revoke, or Limit SAP access. The Air Force CAO, Wright-Patterson AFB, OH is the authority to grant, deny, suspend, revoke, or limit SAP access eligibility.

A4.9. Officials Authorized to Issue Interim Clearances. Commanders have the authority to grant interim security clearances.

A4.10. Officials Authorized to Designate Nonappropriated Fund Positions of Trust. HRO managers designate these positions within their jurisdiction. See AFI, 34-301, *Nonappropriated Fund Personnel Management and Administration.*

Attachment 5

STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD

A5.1. Personnel Security Appeal Board.

A5.1.1. Responsibilities:

A5.1.1.1. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) has oversight of the Personnel Security Appeal Board (PSAB).

A5.1.1.2. The PSAB:

A5.1.1.2.1. The PSAB is the appeal authority for security clearances and SCI access (see Chapter 11). Determinations made to deny or revoke security clearances shall be made IAW DOD 5200.2-R, this AFI Chapter 8, and "BY AUTHORITY OF THE SECRETARY OF THE AIR FORCE."

A5.1.1.2.2. The PSAB is comprised of three members.

A5.1.1.2.3. The PSAB President will be an HQ USAF/XO representative and will serve as a permanent member. An attorney from HQ USAF/JA and a security official from HQ USAF/XOFI will be permanent members. A medical advisor from HQ USAF/SG will be available to the board at two-year intervals. The members will be briefed on and familiar with the personnel security clearance process.

A5.1.1.2.4. Minimum grade 0-5/GS-14. In cases where the appellant is at or above the grade of military 0-5 or GM/GS-14, at least one member of the board will be equivalent or senior in grade to the appellant.

A5.1.1.2.5. The President executes board responsibilities as outlined in DOD 5200.2-R, Appendix M and this AFI.

A5.1.1.2.6. The PSAB convenes upon receipt of appeal cases.

A5.1.1.2.7. The PSAB president notifies appellants, in writing, of the decision generally within 60 days of receipt of the appeal (with no personal appearance) or 30 days of receipt of the Administrative Judge's recommendation (with a personal appearance). The notice will include a statement that the PSAB decision is final and no other appeal rights are authorized. If SCI is involved, the notice will specify the status of the access to SCI, in addition to the security clearance. A copy of the board's final decision is forwarded to the CAF.

A5.1.1.3. The CAF:

A5.1.1.3.1. Provides operational support to SAF/AA and the PSAB.

A5.1.1.3.2. Forwards the appeal case file to the PSAB President and includes a case summary on all cases to assist the board members' review.

A5.1.1.3.3. Sends membership letters to designated functional representatives to serve on the board.

A5.1.1.3.4. Provides the Defense Office of Hearings and Appeals (DOHA) with the case files upon request.

A5.1.1.3.5. Updates the DCII and AMS.

A5.1.1.3.6. Maintains the redacted file for the PSAB. AFI 37-131 applies when requests for information are received.

A5.1.1.3.7. Provides SAF/AA with a report quarterly that tracks the decisions on appeal cases.

Attachment 6

SAMPLE WAIVER OF PRE-APPOINTMENT INVESTIGATIVE REQUIREMENTS

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR (Servicing Civilian Personnel Flight)

FROM: Unit of Assignment Full Address

SUBJECT: Waiver of Preappointment Investigative Requirements

In accordance with AFI 31-501, paragraph 3.1, I have waived the investigative requirements and give authority to fill a critical sensitive (or noncritical sensitive) position prior to completion of the personnel security investigation. (Name of individual, SSAN) has been selected for the position of (fill in), grade, and office symbol.

Appointment prior to completion of the investigation is necessary to accomplish (fill in) function in support of national security.

Temporary changes will be made in duties or work situation to preclude the person from access to classified material or information before completion of the required investigation.

Commander's Signature Block

Attachment 7

SAMPLE MEDICAL CERTIFICATION TO THE COMMANDER OF INDIVIDUAL FOR PRESIDENTIAL SUPPORT PROGRAM

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Commander of Individual Being Nominated)

FROM: Medical Officer Full Address

SUBJECT: Medical Certificate

(One of the following actions have been taken:)

This certifies a competent medical authority reviewed the medical records regarding (grade, full name, SSN of individual) and no physical or mental disorder is noted in the record that could adversely affect the individual's judgment or reliability. The medical authority who reviewed the records is (name) and may be contacted at (telephone number).

OR

This certifies a competent medical authority reviewed the medical records regarding (grade, full name, SSN of individual) and found the following potentially disqualifying information that could adversely affect the individual's judgment or reliability: (i.e., drug abuse, alcohol abuse, mental or emotional problems, etc). The medical authority who reviewed the records is (name) and may be contacted at (telephone number).

Medical Officer's Signature Block

NOTE: If a commander needs an interview with the medical authority to discuss the findings in order to base a nominating decision, the medical authority provides a statement of that interview to the commander. Any statements will be kept with the certificate.

Attachment 8

SAMPLE COMMANDER'S NOMINATION TO CHIEF, SERVICING SECURITY ACTIVITY FOR A PRESIDENTIAL SUPPORT POSITION

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR CHIEF, SERVICING SECURITY ACTIVITY

FROM: Commander Full Address

SUBJECT: Presidential Support Nomination for (Job Title) by (Full Name, Rank/Grade, SSAN)

The attached personnel security investigation package on (enter name, rank or civilian grade, SSAN), United States Air Force (or company name of contractor) has been completed in accordance with DOD Instruction 5210.55 and AFI 31-501. It is forwarded for further processing (Atchs 1 & 2).

(Enter name) is being nominated for (state initial or continued assignment) to (identify the specific presidential support activity) as a (identify the individual's specific duty assignment, i.e., aviation maintenance technician, security force, steward, rotor blade examiner, driver, etc).

These duties are identified as (Category One) or (Category Two) requiring a favorably completed Single Scope Background Investigation (SSBI) or (Category Three) requiring completion of a favorable National Agency Check, local agency check and credit check (NACLC).

I have personally reviewed the individual's records as follows and there is no derogatory information that would disqualify the nominee from selection:

(1) efficiency and or fitness reports file reflects the individual has demonstrated consistent high standards of performance;

(2) military personnel records or civilian official personnel folder, or contractor personnel records reveal no derogatory information; and

(3) local security files reveal no derogatory information.

I have on file the certificate from a competent medical authority that certifies no physical or mental disorder is noted that could adversely affect the individual's reliability or judgment. I have no knowledge of, and base law enforcement records do not reveal, any delinquency or criminal activities on the part of the nominee. No actions are pending to deny, revoke, or withdraw any security clearance or access.

(Enter name) is recommended for assignment to (enter unit/company and location) and duties (enter job title) for which nominated. (Justify the recommendation if derogatory information is in the records. Specifically identify all reasons for a recommendation that a contractor employee shall not be selected for the particular position in question).

Our POC is (name and (telephone number).

Commander's Signature Block

Attachments:

1. EPSQ Disk & 1 Signed Original
2. FBI Fingerprint Card

Attachment 9

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, MEMORANDUM TO 497 IG/INS FOR PROCESSING OF PRESIDENTIAL SUPPORT PROGRAM NOMINEE

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR 497 IG/INS

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Request for Processing Presidential Support Program Nominee

The attached Commander's Nomination Memorandum on (enter name, rank or civilian grade, SSAN), United States Air Force (or company name of contractor) has been processed in accordance with DOD 5210.55 and AFI 31-501. It is forwarded for your further processing.

The commander (name and unit) has recommended (enter name, rank or civilian grade, SSAN) for assignment to (or continued assignment) (enter unit/company and location) and duties to an authorized Presidential Support position (enter job title).

The commander has certified the records of (enter name, rank or civilian grade, SSAN) reveal no disqualifying information.

The required investigation (NACLC or SSBI) was submitted to the Defense Security Service or the Office of Personnel Management on (date).

Our POC is (name, grade, telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

Commander's Nomination Memorandum (attachments withdrawn)

Attachment 10

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, NOTIFICATION TO THE SERVICING MEDICAL FACILITY OF THE INDIVIDUAL APPROVED FOR PRESIDENTIAL SUPPORT DUTIES

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Servicing Medical Facility)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Assignment of Presidential Support Duties

The following individual has been approved for assignment to a Presidential Support position on (date).

(name, rank, grade, SSAN, unit, office symbol)

Request the individual's medical records be marked and monitored during this assignment in accordance with the instructions in AFI 31-501, *Personnel Security Program Management* and use of AF Form 745, Sensitive Duties Program Record Identifier. See AFI 41-210, *Patient Administration Functions.* Notify the individual's commander or designated representative and this office when a significant effect on the individual's suitability to perform Presidential Support duties is expected as a result of medical, dental, or mental health treatment or medication, and if drug or alcohol abuse is suspected.

We will notify you to terminate monitoring when the individual is no longer assigned to Presidential Support duties.

Our POC is (name, grade, and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 11

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, REQUEST FOR EVALUATION OF CONTINUED SECURITY CLEARANCE TO COMMANDER

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Unit Commander)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Evaluation of Continued Security Clearance

The attached unfavorable and or derogatory information has been developed concerning the above member of your organization. Please review this information and determine on the basis of the facts available, if it is in the interest of national security to establish a Security Information File (SIF) and whether or not to suspend access to classified information/unescorted entry to restricted areas while such information is resolved. Your review of the security standard criteria in AFI 31-501, Chapter 8, and DOD 5200.2-R, paragraph 2-200 will guide your decision.

Upon completion, please provide your decision and rationale for or against SIF establishment.

My POC, (name and telephone number) stands ready to assist you. Please respond NLT (date).

Chief, Servicing Security Activity Signature Block

Attachments(s):

1st Ind, (date)

TO: Unit HQ USAF/SFAI

I have reviewed the referred available unfavorable information concerning subject and do not believe the suspension of access to classified information and or unescorted entry is warranted. My rationale for this decision is___(explain)_____. Consequently, I've determined this case doesn't meet the purview of AFI 31-501 for SIF establishment. This individual's continued access and or entry is in the best interest of national security. Should additional unfavorable and or derogatory information become available, I will reevaluate my decision. I have or have not coordinated this decision with the JA.

OR

I have reviewed the referred unfavorable information concerning the subject. I have determined the derogatory and or unfavorable information concerning subject falls within the criteria of AFI 31-501, Chapter 8. A SIF has been established, please set up a folder and maintain a SIF as outlined in AFI 31-501, Chapter 8.

I have or have not withdrawn (suspended) subject's access to classified information and or unescorted entry to restricted areas. Attached as applicable is the:

a. AF Form 2583, **Request for Personnel Security Action**. (This form is used to document Special Access, i.e., NATO, CNWDI, SIOP, etc.)

b. AF Form 2586, **Unescorted Entry Authorization Certificate**, stamped by Pass & Registration Section, reflecting restricted area badge was returned.

c. AF Form 2587, **Security Termination Statement**.

d. Notification of suspension of access.

My rationale for this decision is: Subject's current situation (conduct, incident, status, pending administrative or judicial action, etc.). Previous disciplinary problems/incidents and action taken, if any. Subject's duty performance. Any evaluations the subject has received. Any other pertinent information. Subject's retainability in the Air Force.

To assist in resolving this case I've taken the following actions: requested investigation, referred individual for evaluation, etc. We'll keep your office informed of any developments and or changes.

Our POC is (name and telephone number):

Commander's Signature Block

Attachment(s)

Attachment 12

SAMPLE REQUEST TO ESTABLISH A SECURITY INFORMATION FILE (SIF)

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR SFS/SFAI

FROM: Commander Full Address

SUBJECT: Request Establishment of Security Information File (SIF), re**: (Last Name, First, Middle, Rank, SSAN)**

Request a SIF be established on **(Individual)** and processed IAW AFI 31-501, *Personnel Security Program Management.*

I have become aware of the Subject's involvement in (specify situation). After review of DOD 5200.2-R, paragraph 2-200, Appendix I, and AFI 31-501, Chapter 8, it is determined that further evaluation is needed to determine the subject's eligibility to retain access to classified information/unescorted entry to restricted areas.

(One of the following actions have been taken:)

(SUBJECT) has been placed in a nonsensitive position and all access to classified information and or unescorted entry to restricted areas has been **withdrawn (suspended)** in accordance with AFI 31-501.

Or

(SUBJECT) will **continue** access to classified information/unescorted entry to restricted areas in accordance with AFI 31-501. **(ANY OF THE FOLLOWING AS PERTINENT).**

Please notify the 497 IG/INS (CAF) of the suspension (or continued access to classified information).

There is a Report of Investigation (ROI). Name of agency conducting the investigation. Date of ROI.

Subject has been referred to (when applicable):

Mental Health for an evaluation Date of referral.

Subject was given disciplinary action for this incident. Type of disciplinary action. (e.g., Article 15)

A Court-Martial is projected for this individual: **(Date)**

Subject was placed in appellate leave status: **(Date)**

The subject's present Date Eligible Retirement or Separation (DEROS) date is.

We **(do/do not)** intend to discharge the subject in accordance with AFI 36-3206, *Administrative Discharge Procedures for Commissioned Officers*, or AFI 36-3208, *Administrative Separation of Airmen.*

I will provide your office with status updates. Our POC is (name and telephone number).

Commander's Signature Block

Attachments:

1. Adverse Security Determination
2. AF Form 2583 (Only if special access is being withdrawn, not to include SCI)
3. AF Form 2586
4. AF Form 2587

Attachment 13

SAMPLE COMMANDER NOTIFICATION TO INDIVIDUAL OF SIF ESTABLISHMENT AND SUSPENSION OF ACCESS TO CLASSIFIED INFORMATION

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Individual Concerned)

FROM: Commander Full Address

SUBJECT: Notification of Suspension of Access

You are hereby notified that a security determination has been made to suspend your access to classified information/unescorted entry into restricted areas. This action is being taken because of your alleged (be as specific as protection of sources allows and national security permits.)

If you wish to provide a rebuttal reply to this determination, I must receive it no later than 72 hours (unit establishes time frame) after your receipt of this notification.

If you choose to reply, a written response to your submission will be made dealing with the points or questions you raise.

A Security Information File will be established. When all final actions in this case have been completed, I will evaluate the incident(s) and make a security recommendation. The 497 IG/INS (CAF) will make the final security determination concerning your reinstatement of clearance eligibility.

Our POC is (name and telephone number).

Commander's Signature Block

cc:

Servicing Security Activity

1st Ind, (Individual Concerned)

TO: (Individual's Commander or Staff Agency Chief)

Receipt acknowledge (Date)

I (do/do not) intend to submit a written reply within 72 hours. (Unit establishes time frame)

Individual's Signature Block

cc:

Servicing Security Activity

Attachment 14

SAMPLE COMMANDER NOTIFICATION TO INDIVIDUAL OF SIF ESTABLISHMENT WITH CONTINUED ACCESS TO CLASSIFIED INFORMATION

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Individual Concerned)

FROM: Commander Full Address

SUBJECT: Notification of Decision to Establish a Security Information File with Individual Continuing Access to Classified Information

You are hereby notified that a security determination has been made to establish a Security Information File. This action is being taken because of your alleged (be as specific as protection of sources allows and national security permits.)

However, I have determined your current access to classified information may continue until further notice.

If you wish to provide a written rebuttal reply to this determination, I must receive it no later than 72 hours (unit establishes time frame) after your receipt of this notification.

If you choose to reply, a written response to your submission will be made dealing with the points or questions you raise.

When all final actions in this case have been completed, I will evaluate the incident(s) and make a security recommendation. The 497 IG/INS (CAF) will make the final security determination concerning your security clearance eligibility.

Our POC is (name and telephone number).

Commander's Signature Block

cc:

Servicing Security Activity

Attachment 15

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, NOTIFICATION TO COMMANDER OF SIF ESTABLISHMENT

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Commander of Subject)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Establishment of a Security Information File (SIF) RE: (Name of Subject)

A SIF has been established on subject individual within your organization IAW AFI 31-501, Chapter 8.

The following documents have been placed in the file:

a. A copy of your letter, dated (date) Subject: Establishment of a Security Information File.

b. A copy of the SIF establishment notification to 497 IG/INS (CAF).

c. A copy of my notification to the (Commander, Support Group), informing him/her of establishment of the file and the contents therein.

The file will be maintained by this office until all local actions are complete. The file will then be forwarded to the 497 IG/INS for a final security clearance determination.

We will request written opinions from base level staff agencies, such as legal, medical, mental health, security forces, and personnel on your behalf. If a Special Investigative Inquiry is necessary, we will request the CAF have DSS conduct one accordingly.

Please provide us with the following recommendation and or documentation for incorporation into the file:

a. Copies of any investigative reports (e.g., AFOSI, DSS, local security forces investigations, FBI, etc.) that will have a bearing on the final resolution of the case.

b. Summary of appropriate portions of subject's Unfavorable Information File (UIF), if any, that may have a bearing on the final adjudication of the case.

c. Correspondence and forms related to withdrawal, revocation, suspension of special access, or correspondence documenting a commander's recommendations relating to withdrawal or suspension of special access or clearance. If not already accomplished, the AF Form 2586, **Unescorted Entry Authorization Certificate**, must be submitted to show that the AF Form 1199A/B/C/, **Restricted Area Badge**, has been turned over to the Pass & Registration Section. In addition, an AF Form 2587, **Security Termination Statement**; and an AF Form 2583, **Special Access Certificate**; must be supplied for inclusion in the SIF.

Please advise this office of any changes and or status reports in order that we may keep the CAF informed of the actions taken. The first update is due to our office by (date) (determined by security activity) and at (number of days) day intervals until the case file is closed.

Once all required documentation is provided, we will provide you with the completed file for your review and final recommendation for closure. We will then forward it to the CAF for final adjudication.

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 16

SAMPLE SIF CUSTODIAN CHECKLIST ITEMS

1. Identifying Data: NAME, RANK, SSAN, OFFICE SYMBOL

2. Establishment Date: DATE, BY (AUTHORITY), REASON, SOURCE: (If appropriate)

3. Review SENTINEL KEY Data: CLEARANCE/SAR CODE, INVESTIGATION TYPE, SPECIAL ACCESS

4. SIF request letter to Chief, Security Activity. (***NOTE:*** Discuss with Chief, Servicing Security Activity if establishment may compromise an ongoing investigation.)

5. Evaluation letter to unit commander based on unfavorable information developed within SF channels, e.g., DD Form 1569, AF 3545, OSI report, PRP suspension/decertification, etc.

6. Adverse action determination letter presented.

7. Moved to nonsensitive position, access to classified/unescorted entry to restricted areas suspended, peers/supervisors briefed.

8. SIF establishment notification to the 497 IG/INS (CAF).

9. Installation Commander notified of SIF establishment.

10. Relinquish AF Form 1199, **USAF Restricted Area Badge**, to Pass and Registration.

11. AF Form 2583, **Request for Personnel Security Action**, used as a special access certificate, withdrawn.

12. AF Form 2586, **Unescorted Entry Authorization Certificate**, annotated.

13. AF Form 2587, **Security Termination Statement**, completed.

14. Request appropriate Servicing Security Activity, AFOSI, or DSS investigation. (Ensure copies of all reports are provided to Servicing Security Activity for SIF inclusion.)

15. Direct and ensure subject receives assistance and counseling as necessary from such agencies as mental health, social actions, chaplains, etc.

16. Provide status reports, via CAVS or memorandum to the 497 IG/INS (CAF).

17. Judicial/administrative actions complete.

18. Obtain written opinions requested and received from appropriate staff agencies, e.g. DP, SF, JA, SG, etc.

19. Forward SIF to gaining installation Chief, Servicing Security Activity based on PCS orders. Information copy to the 497 IG/INS (CAF).

20. Completed file with any written suspension response from subject transmitted to the CAF.

21. Maintain all documentation necessary to complete the SIF.

Attachment 17

SAMPLE NOTIFICATION TO 497 IG/INS OF SIF ESTABLISHMENT WHEN INDIVIDUAL MAINTAINS ACCESS

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR 497 IG/INS (CAF)

229 Brookley Ave

Bolling AFB, DC 20332-7040

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Establishment of Security Information File (SIF), re: (name of subject)

The commander of (identify unit) has requested establishment of a SIF on (name and SSAN) due to (specify issue as outlined in the adjudication guidelines, DOD 5200.2-R). At this time the commander has authorized the individual to maintain current access to classified information, to include SCI access.

The SIF was established on (date).

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 18

SAMPLE SIF ESTABLISHMENT NOTIFICATION TO INSTALLATION COMMANDER

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR (Installation Commander)
FROM: Chief, Servicing Security Activity Full Address
SUBJECT: Establishment of Security Information File (SIF)

The following information is provided to inform you of the establishment of a SIF:

a. Name:
b. Rank:
c. Organization:
d. Reason for SIF Establishment:
e. Date SIF was established by commander or staff agency chief:

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 19

SAMPLE REQUEST FOR REVIEW AND WRITTEN OPINION

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR (DP, SF, JA, SG, as determined by the nature of the case)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Review and Written Opinion - Security Information File (SIF)

The Commander of (organization) has requested this office to establish a SIF on (individual and SSAN).

AFI 31-501, Chapter 8, request your review and written opinion concerning the attached SIF. Please review the file and provide your professional opinion and or recommendation concerning whether this individual should or should not retain a security clearance. This information is required to assist me and 497 IG/INS (CAF) in determining if this person's clearance is in the best interest of the Air Force and national security.

In addition, please review any other pertinent records available in your office and advise if there is any additional information that would warrant the continued denial of access to all classified information and unescorted entry to all restricted areas. A denial or revocation will cover classified at all levels.

Please return the entire package with a record of your review comments and recommendation not later than (10 working days).

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

SIF, RE: (Name of Subject)

cc:

Commander (organization)

Attachment 20

SAMPLE SIF TRANSFER MEMORANDUM TO GAINING SECURITY ACTIVITY

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR (Gaining Chief, Security Activity)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Transfer of Security Information File (SIF), ref: (Name of Subject, Rank, SSAN)

The attached SIF is forwarded in accordance with AFI 31-501, Chapter 8.

The subject has received orders for Permanent Change of Station (PCS) to your installation, with a report date of (date).

A copy of this transmittal letter is being forwarded to the 497 IG/INS (CAF) for information.

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

SIF

cc:

Commander (of subject)

497 IG/INS (CAF) w/o attachment

Attachment 21

SAMPLE RECOMMENDATION TO 497 IG/INS FOR SIF CLOSURE

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR 497 IG/INSAF

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Recommendation for SIF Closure RE: (Name of Subject)

The attached SIF on (name and SSAN of subject) is forwarded for your final adjudication. All final actions in this case completed as outlined below:

a. Mental health evaluation:

b. Completed alcohol and/or drug rehabilitation program:

c. Received financial counseling from:

d. Administrative action taken:

e. Judicial action: (An opinion from staff judge advocate regarding factors used in determination of withdrawal or dismissal of charges when there is evidence the individual engaged in the misconduct. For example, positive urinalysis, but found not guilty through court-martial. Was the finding based on technicalities or evidence?)

f. Add any additional pertinent information.

This individual will be returned to duty and or cross trained/separated/placed in appellate leave status.

The individual's commander (name, organization, telephone number) recommendation for (favorable closure and or revocation of security clearance) is included in the SIF.

Our POC is (name and DSN telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

SIF (if applicable)

cc:

Commander (of subject)

Attachment 22

INSTRUCTIONS FOR MAILING EPSQ DISKETTE TO DSS

A22.1. Use the following procedures for mailing EPSQ diskette to DSS:

A22.1.1. Create, validate, print, certify, and prepare the EPSQ file before copying to a diskette.

A22.1.2. Certification and preparation of EPSQ data is accomplished in the Communications Utility of the EPSQ software. Files that have been properly prepared will appear in the following format: file name followed by .z20, e.g.webster.z20.

A22.1.3. Submit up to five Subject and Security Officer forms per 3.5" high density, 1.4-mb diskette.

A22.1.4. Label the diskette with the following:

A22.1.4.1. Return Address.

A22.1.4.2. Security Officer's name or other designated point of contact.

A22.1.4.3. Telephone number (DSN).

A22.1.4.4. Last name(s) of the Subject(s) whose EPSQ(s) is (are) contained on the diskette.

A22.1.5. Place the signed copy of the Authorization for Release of Information (and fingerprint cards(s), if applicable) in the same envelope as the diskette; mail them, with self-addressed envelope to: Defense Security Service, ATTN: EPSQ Diskette Processing, P.O. Box 46060**,** Baltimore, MD 21240-6060.

A22.1.6. The diskettes will not be returned to the authorized requester.

Attachment 23

INSTRUCTIONS TO COMPLETE AF FORM 2583, REQUEST FOR PERSONNEL SECURITY ACTION

Table A23.1. Instructions to Complete AF Form 2583, Request for Personnel Security Action.

LINE	A	B	C
	To Complete		Enter
	Section	Item	
1	I	1	last, first, middle, and maiden name to agree with military or employment records; if not, explain in Section VII. If no middle name, or initial only, enter "NUN" or "IOU," respectively. Also, enter the maiden name for female personnel.
2		2	the unit designation. When the form pertains to non-DOD personnel, enter the unit designation of the sponsoring activity.
3		3	grade. Do not change this entry after the form is filed and a change in grade occurs.
4		4	social security number.
5		5	an "X" in only one block.
6		6	year, month, and day of birth, in that order. For example: 20000210
7		7	city, state, and country of place of birth.
8	II	8	an "X" in only one block.
9		9	an "X" in applicable blocks. Check only the highest level of clearance, access, or entry requirement. (See Note 1 for Limited Access Authorization requests.)
10	III	10	activities required to search their records for possible derogatory information from a personnel security standpoint. Medical and security police activities are usually the agencies required to take this action (see Notes 2 and 3).
11		11	unit of assignment. Also include the telephone number of the requester, to ensure that immediate contact can be made in the event questions should arise.
12		12	date when requester signs the form.
13		13	typed name, grade, and title of the unit commander or staff agency chief, or security manager when delegated this authority.
14		14	self-explanatory. The signature certifies actions in Note 4 have been complied with.
15	IV	15	self-explanatory (see Note 3).
16		16	date when the check is completed.
17		17	typed name and grade of base director of medical services (see Note 5).
18		18	self-explanatory.
19	V	19	see Notes 2 and 6.
20		20	date when the check is completed.
21		21	typed name and grade of the chief of servicing security activity, or designees, in the security clearance function or reports and analysis section.
22		22	self-explanatory.
23	VI	23	an "X" in applicable blocks. In spaces provided, also include the classification level the member requires access to. Except for sensitive compartmented information (SCI) and the PRP, use Section VII to add any other special access program not covered. SCI is not entered, because the MAJCOM or FOA SCI billet manager centrally manages personnel authorized this access. PRP is not entered, since separate forms are used to administer this program.
24		24	self-explanatory.
25		25	enter name, grade, and title of one-time access approving official.
26		26	self-explanatory.
27		27	date when access to special program information is granted.
28		28	typed name, grade, and title of special access program certifying official. Only officials authorized by the governing directive may certify this entry. Use Section VII to show coordination action when two or more special access programs are involved, and the same official grants all access.
29		29	self-explanatory.
30	VII	30	self-explanatory (see Note 7).

NOTES:

1. Send a request letter through channels to the approving authority when non-US nationals or immigrant alien personnel require limited access to Secret or Confidential defense information or unescorted entry to PL 1, 2, or 3 restricted areas.

2. Complete items 10 through 14 when an investigation or a security clearance is required. The LFC is not required when recording special access program authorizations, unless specified in the governing directive. This guidance also applies to sections IV and V.

3. If the individual records derogatory information in Section VII, promptly notify the requester and security information file custodians. This action determines if re-adjudication of the person's security clearance is necessary by the CAF. This guidance also applies to Section V.

4. Ensure the request process includes a review of SK for evidence of an UIF concerning the member. Also, review personnel records to determine if derogatory information exists from a personnel security standpoint. Check personnel records to confirm other data, such as employment or military service as listed on SF Form 86, when necessary. Persons designated to sign Item 14 of the form must take or confirm these actions. Enter results of these reviews in Section VII.

5. Note that this authority may be delegated to other medical staff personnel who may review medical records and form professional opinions based on the information being evaluated. If no medical records are on file (as for many civil service

employees) annotate the form to that effect. The DD Form 1879 then shows no local medical records were checked and DSS agents check the records.

6. Review the records of the security clearance function and reports and analysis section. If a SIF exists, deny the requested personnel security action pending completion of adjudication actions. In these cases, also enter in Section VII that a SIF exists. Also, review the remarks section for any other derogatory information reported and evaluate the need to establish a SIF for further adjudication. Enter results of this evaluation in Section VII.

7. Annotate Section VII to reflect what document was used to verify citizenship status.