



**PERSONNEL SECURITY PROGRAM
MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the 3rd Wing WWW site at: <http://infonet/irgs/3wg/3sptg/3cs/scs/scsp/pdl/index.htm>. If you lack access, contact your Publishing Office.

OPR: 3 SFS/SFAP (Mrs. Mae Parker)

Certified by: 3 SPTG/CC (Col T. W. Van Splunder)

Pages: 4

Distribution: F

This supplement applies to all host, associate (participants), and temporary (TDY) organizations on Elmendorf AFB, including the Air National Guard and US Air Force Reserve members and units.

AFI 31-501, 1 August 2000, is supplemented as follows:

3.6. The Civilian Personnel Flight ensures a pre-employment waiver is completed by commanders on all new employees who are designated to fill Non-Critical Sensitive and Critical Sensitive positions, prior to the individual reporting for work. The individual's unit of assignment will provide a copy of the pre-employment waiver letter to 3 SFS/SFAP. A pre-employment waiver does not authorize the individual access to classified information, automated information systems (AIS), or a restricted area badge. The individual must have a security clearance for access to classified information or a favorable investigation for access to AIS and unescorted entry to restricted areas.

3.11. Commanders may grant interim security clearances, through 3 SFS/SFAP, for Top Secret and Secret access to classified information when the requirements of DoD 5200.2-R, Department of Defense Personnel Security Program, paragraph 3-401, have been met. Interim clearances may be revoked at any time based on unfavorable information identified in the course of the investigation. Interim clearances should be held to mission essential personnel only and strict scrutiny should be used in granting interims.

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

3.11.1.1. The 3 SFS/SFAP must verify a favorable Entrance National Agency Check (ENTNAC), National Agency Check (NAC), National Agency Check with Written Inquires (NACI), National Agency Check Plus Written Inquires and Credit Check (NACIC), National Agency Check, Local Agency Checks, and Credit Checks (NACLC), or Access National Agency Check with Written Inquiries and Credit Check (ANACI) has been completed.

3.11.1.2. Unit security manager accomplishes an AF Form 2583, *Request for Personnel Security Action*, requesting local files checks of personnel records (military personnel information file (PIF) and civilian

official personnel file (OPF)), Security Forces, medical records (Physical Exams, Mental Health, and Family Advocacy), and other security records as appropriate.

3.11.1.3. Unit commander or staff agency chief must conduct a review of the individual's Electronic Personnel Security Questionnaire (EPSQ)/SF 86, *Questionnaire for National Security Positions*, and local files.

3.11.1.4. The 3 SFS/SFAP must receive a confirmed receipt of a single scope background investigation (SSBI) request submitted to Defense Security Service (DSS) or Office of Personnel Management (OPM).

3.11.1.5. (Added) (3 WG). The unit commander must favorably review all information provided, complete an additional AF Form 2583 requesting the interim clearance be granted, and route the interim package through 3 SFS/SFAP for processing and granting of the interim clearance.

3.11.1.6. (Added) (3 WG). The unit security manager will verify within 5 duty days, using Sentinel Key, to ensure the interim clearance has been granted.

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

3.11.2.1. Unit security manager accomplishes an AF Form 2583 requesting local files checks of personnel records (military personal information file (PIF) and civilian OPF), Security Forces, medical records (Flight Medicine, Mental Health, and Family Advocacy), and other security records as appropriate.

3.11.2.2. Unit commander or staff agency chief must conduct a review of the individual's EPSQ/SF 86, and local files.

3.11.2.4. The 3 SFS/SFAP must verify an open NAC or a confirmed receipt of a NACLIC or ANACI request at DSS or OPM.

3.11.2.5. (Added) (3 WG). The unit commander must favorably review all information provided, complete an additional AF Form 2583 requesting the interim clearance be granted, and route the interim package through 3 SFS/SFAP for processing of the interim clearance.

3.11.2.6. (Added) (3 WG). The unit security manager will verify in Sentinel Key within five duty days that the Interim clearance has been granted.

3.11.5. (Added) (3 WG). If an individual has an interim clearance granted and the normal security clearance has not been granted by the interim's 12-month point, the entire interim process must be re-certified. The individual must have local files checks accomplished and documented on the AF Form 2583. A copy of the AF Form 2583 and a memorandum from the unit commander stating desire to extend the interim security clearance must be forwarded to 3 SFS/SFAP.

3.11.6. (Added) (3 WG) When an individual has been granted an interim clearance at a previous location and it is recorded in Sentinel Key, the gaining unit commander will review the individual's SF 86 and local PIF. The unit commander will complete a memorandum for record indicating desire to honor the previously granted interim. Forward a copy of the SF 86 and memorandum to 3 SFS/SFAP for the record.

3.24.7. Follow the procedures for interim Secret clearance outlined in paragraph 3.11.2, this instruction, for granting interim access to AIS and unescorted entry to restricted areas holding Protection Level 2 (PL2) and Protection Level 3 (PL3) resources. For access to Protection Level 1 (PL1) resources, the individual must have a security clearance or favorable completed investigation.

5.1.1. The unit security managers will produce a clearance and access verification system (CAVS) roster by the 10th of each month. The security manager will verify all the information on the CAVS roster is correct and take actions to correct any discrepancies.

5.1.2. (Added) (3 WG). The unit security manager will produce a periodic review (PR) report for their unit by the 10th of each month and notify the individuals within 3 duty days that they are due for a personnel security investigation (PSI). Unit security manager will develop a tracking system of individual notified to complete the EPSQ. Security manager will notify the commander and supervisor of individuals who fail to meet their suspense.

5.1.3. (Added) (3 WG). PSI packages will be received at 3 SFA/SFAP office no later than 30 days from the date the individual is notified to complete the PSI.

5.1.3.1. (Added) (3 WG). The 3 SFS/SFAP will not accept PSI paperwork when dates on the AF Form 2583 are older than 30 calendar days. SFs 85, *Questionnaire for Non-Sensitive Positions*, 85P, *Questionnaire for Public Trust Positions*, and 86, *Questionnaires for National Security Positions*, or FD 258, *FBI Fingerprint Card*, will not be accepted if the individual's releases of information pages signatures/dates are more than 90 days old.

5.1.3.2. (Added) (3 WG). Items required with PSI: Primary or alternate unit security manager will quality check and review all PSI packages for completion prior to submittal to 3 SFS/SFAP and include documents identified below.

5.1.3.2.1. Printed EPSQ (current version) of SF 86. **NOTE:** Two signed copies.

5.1.3.2.2. All releases of information forms signed.

5.1.3.2.3. AF Form 2583, two copies.

5.1.3.2.4. DD Form 1879, *DoD Request for Personnel Security Investigation* (Top Secret Requests Only), two copies.

5.1.3.2.5. OPM Cover sheet, completed and signed, two copies.

5.1.3.2.6. EPSQ diskette w/password: (Only EPSQ will be used as the password).

5.1.3.2.7. Error-free validation report.

5.1.3.2.8. FD 258 (for initial personnel security investigations (PSI) and Special Access Programs), one card.

5.1.3.2.9. MPF FM 015, *Outbound Assignment Memorandum (as applicable for permanent change of station (PCS) move)*.

5.1.3.2.10. Security access requirement (SAR) code change memorandum from unit commander reflecting upgrade in access requirement.

5.1.3.3. (Added) (3 WG). Items required for AAFES and contractor employees (positions of trust, AIS, and restricted area badge issue) are:

5.1.3.3.1. AF Form 2583, two copies.

5.1.3.3.2. OPM Cover sheet, completed and signed, two copies.

5.1.3.3.3. Printed EPSQ (current version) of SF 85P, two copies.

5.1.3.3.4. EPSQ diskette w/password: EPSQ

5.1.3.3.5. Error-free validation report.

5.1.3.3.6. SF 87, *US Civil Service Commission Fingerprint Card*, one card.

5.1.3.4. (Added) (3 WG). Non-Appropriated Funds (NAF) employees PSI are submitted by the NAF Human Resource Office. Fingerprints can be obtained at the 3rd Security Forces Squadron, Pass & Registration Section. Call 552-3202, for hours of printing.

5.2.1. The 3 SFS/SFAP (Personnel Security Office) is the designated “authorized requestors” for all AF clearance transactions for Elmendorf AFB. **EXCEPTIONS:** NAF, Civilian Personnel, and 381 IS, are also authorized requestors.

7.1.2.2. This review will be conducted in January each year and reported via memorandum to 3 SFS/SFAP no later than 15 February following the review.

7.5. The unit security manager will verify via sentinel key all unit personnel who are in access positions and/or have access to restricted areas have signed a SF 312, *Classified Information Non Disclosure Agreement*. If an individual has not signed the SF 312, the unit security manager will have the individual sign a SF 312 and update sentinel key to reflect the date the individual signed the SF 312 and mail the original to the appropriated address identified in AFI 31-401, *Information Security Program Management*.

8.2.1.3. Unit commanders must determine whether or not to establish a security information file (SIF) within 20 days from notification of unfavorable information regardless of whether the notification derived from 3 SFS/SFAP, internally, or another agency. However, if the commander has sufficient reason to doubt the validity of the unfavorable information he/she can request an extension, up to 45 days, for the decision to establish a SIF. The extension must be requested through 3 SFS/SFAP.

8.2.2.8. Commanders must provide updates to 3 SFS/SFAP on all established SIFs within their unit by the 45th day and request closure of the SIF by the 90th day of the SIF being open. If the SIF cannot be closed within 90 days, the commander must request an extension of the SIF through 3 SFS/SFAP who in-turn will notify the Air Force Central Adjudication Facility (AFCAF) and request an extension beyond their 120-day suspense.

8.2.3.1.1. (Added) (3 WG). Unit Commanders, First Sergeants, and Staff Agency Chiefs must confer with the unit security managers when derogative information arises and falls within the guidelines set fourth in AFI 31-501, paragraph, 8.2.1.3.1. and DoD 5200.2-R, Chapter 2, paragraph 2-200.

8.6.3. The 3 SFS/SFAP is the 3 WG point of contact.

DOUGLAS M. FRASER, Brigadier General, USAF
Commander