



**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: 21 SFS/SFAP (TSgt Dale Campbell)

Certified by: 21 SFS/SFA (Ms. Amanda Race)

Pages: 4

Distribution: F

The OPR for this supplement is 21 SFS/SFAP (TSgt Dale Campbell). This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-501, *Personnel Security Program Management*, 1 August 2000, and Air Force Space Command (AFSPC) Supplement 1, 3 February 2003. This supplement provides a baseline requirement for managing the Personnel Security Program. It applies to all serviced Peterson AFB and Cheyenne Mountain AFS host and tenant units. It does not apply to the US Army Space and Missile Defense Command or the Air Force Office of Special Investigations (AFOSI). Maintain and dispose of records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule* (will become AFMAN 33-322 Vol. 4).

1.1.2. All waiver requests must be forwarded through 21 SFS/SFAP.

1.3. **Definitions.** The term “commander” also includes “director”.

3.1. **Authority to Designate Sensitive Positions.** 21 SFS/SFAP will verify security access requirements in the Joint Personnel Adjudication System (JPAS). If the subject requires a Single Scope Background Investigation (SSBI) or an SSBI periodic reinvestigation (SBPR) and the appropriate security access is not indicated in JPAS, the unit is required to submit proof that the individual requires the investigation. A copy of the organization’s unit manning document with the subject’s position highlighted or a letter signed by the commander are acceptable forms of proof.

3.1.1. If the subject’s commander does not respond, 21 SFS/SFAP will forward a security information file (SIF) option letter to the installation commander. If the subject’s commander declines to establish a SIF and the subject does not submit an investigation, 21 SFS/SFAP will forward a SIF option letter to the installation commander.

3.1.2. Security managers must certify in writing that they have reviewed the subject’s personnel security investigation (PSI) for accuracy.

3.2.1. 21 MSS/DPC is the servicing civilian personnel flight.

3.6.2. 21 MSS/DPC will provide 21 SFS/SFAP copies of all pre-employment waivers. 21 SFS/SFAP will maintain a copy of each waiver until the investigation is adjudicated.

3.11. **Interim Security Clearances.** All interim clearance requests will be forwarded to 21 SFS/SFAP. The interim clearance request must certify that the commander has reviewed the subject's electronic personnel security questionnaire (EPSQ) or Standard Form (SF) 86, **Questionnaire for National Security Positions**. If derogatory information exists, the commander must certify that he/she is aware of the information and is willing to accept the risks associated with the derogatory information. All interim requests must also include a completed AF Form 2583, **Request for Personnel Security Action**. AF Forms 2583 completed within the previous 60 days are acceptable.

3.11.4. 21 SFS/SFAP will document interim clearances in JPAS once all required actions are accomplished and will provide the security manager verification that the interim clearance was granted.

3.12.1. All requests for limited access authority (LAAs) must be forwarded through 21 SFS/SFAP.

3.14.2. Security managers will submit consultant PSIs to 21 SFS/SFAP. The AF Form 2583 must clearly indicate that the subject is a consultant.

3.24.6. 21 SFS/SFAP will submit SF 85P, **Questionnaire for Public Trust Positions**, for contractors requiring unescorted entry to restricted areas to OPM. EPSQ will be utilized to complete the SF 85P.

4.1.1.3. Confirmation with the AFCAF that a valid investigation is on file is no longer required if the investigation information is shown in JPAS.

5.1.1.2.2. The unit's personnel security operating instruction (OI) may be incorporated into an overall unit security OI. At a minimum, the personnel security portion must include individual responsibilities.

5.1.1.2.4. Cheyenne Mountain AFS personnel are exempt from attending Peterson AFB ISPM-hosted security manager meetings. 21 SFS/SFAP will inform 721 SFS/SFA of pertinent issues to be passed along at Cheyenne Mountain AFS ISPM-hosted security manager meetings.

5.1.1.2.6. HQ AFSPC no longer requires the status of all PSIs on a weekly basis. Provide the status on a monthly basis to 21 SFS/SFAP no later than the date established by 21 SFS/SFAP unless otherwise directed.

5.1.2. Security managers will utilize the format provided by HQ AFSPC/SFC through 21 SFS/SFAP.

5.2.1. 21 SFS/SFAP is the authorized requestor and the servicing security activity for Peterson AFB and Cheyenne Mountain AFS. 21 MSS/DPC is the authorized requestor for newly hired civilian employee National Agency Check Plus Written Inquiries and Credit Checks (NACICs), and Access National Agency Check with Written Inquiries and Credit Checks (ANACIs.) All SSBI for newly hired civilian employees will be submitted through 21 SFS/SFAP.

5.6.1. Security managers will document all notifications to individuals requiring an investigation. If an individual refuses to comply, provide the commander all documentation relating to the refusal for SIF establishment. Courtesy copy 21 SFS/SFAP.

5.6.2. Security managers will certify in writing that they have reviewed the subject's PSI for accuracy.

7.1.2.1. Submit position code changes, along with justification for the change, to the servicing manpower office through 21 SFS/SFAP.

7.1.2.2. The review must be documented. It will be reviewed during the organization's annual or biennial information security program review.

7.4. **SENTINEL KEY.** JPAS is the DoD personnel security automated system that contains investigative and clearance data. Sentinel Key is no longer available.

7.4.2.5.4. Security managers must be designated in writing by the commander. Security managers must maintain a JPAS account for effective unit security program management. Forward all other JPAS access requests to 21 SFS/SFAP. 21 SFS/SFAP will either approve the request or justify the disapproval. Typically, JPAS accounts will only be given to non-security managers in situations where the individual supports the installation in some manner that requires the individual to verify security clearances. JPAS accounts will not be given to non-security managers for the sole purpose of convenience to an organization. Disapproved requests may be forwarded to 21 SFS/CC for reconsideration.

7.4.2.8.2. 21 SFS/SFAP will review accounts biannually. All accounts without a security manager appointment letter or valid access request for other individuals will be deleted.

7.6.2. (Added) 21 SFS/SFAP will only release information concerning personnel security investigations to commanders or their appointed unit security manager.

8.2.1.8. 21 SFS/SFAP will request immediate favorable SIF closure when requested by the subject's commander.

8.2.1.10. (Added) Process all correspondence through 21 SFS/SFAP.

8.2.1.11. (Added) Immediately notify 21 SFS/SFAP of retirement, separation, or permanent change of station (PCS) of an individual with a SIF by providing a copy of the applicable orders/personnel actions.

8.7. **Security Clearance Reinstatement.** Process all reinstatement requests through 21 SFS/SFAP.

9.3. **Initial Briefings and Refresher Briefings.** Security managers record indoctrination briefings in JPAS.

9.6. (Added) **Out-Processing Personnel.** Security managers will outprocess individuals PCSing or separating in JPAS.

11.1.4. The Chief, Security Forces (21 SFS/CC) is the information security program manager (ISPM) for Peterson AFB. 21 SFS/SFAP manages the installation personnel security program on his/her behalf.

11.1.5.2. Unit personnel security programs will be evaluated during information security program reviews.

12.5. (Added) **Forms or IMTs Adopted.** SF 86, **Questionnaire for National Security**; AF Form 2583, **Request for Personnel Security Action**; SF 85P, **Questionnaire for Public Trust Positions**.

A2.2.1.3. 21 SFS/SFAP mails all EPSQs to the Office of Personnel Management (OPM). The Defense Security Service (DSS) no longer accepts investigations.

A2.2.1.7. 21 MSS/DPMAR will provide 21 SFS/SFAP copies of military PCS/separation orders.

A2.6. **Local Files Check.** Signatures on AF Form 2583 are valid for 60 days. Security managers will retain AF Forms 2583 until the investigation has been adjudicated.

A2.12.1. All periodic reinvestigations must be mailed or hand-carried to 21 SFS/SFAP. Appointments will only be made for initial investigations. All PRs requiring corrections will be returned to the subject through the security manager.

A2.12.2. Security managers will ensure Secret PRs are submitted to 21 SFS/SFAP at the 9-year 6-month anniversary of the previous investigation for military members in positions coded as “6” on the UMD or civilians occupying noncritical sensitive positions.

A2.12.3. Security managers will ensure Top Secret PRs are submitted to 21 SFS/SFAP at the 4-year 6-month anniversary of the previous investigation for military members in positions coded as “5” on the UMD or civilians occupying critical sensitive positions.

JOHN P. BROOKER, Lt Col, USAF
Chief, Security Forces