

**BY ORDER OF THE COMMANDER  
AIR FORCE SPACE COMMAND**



**AIR FORCE INSTRUCTION 31-501**

**AIR FORCE SPACE COMMAND**

**Supplement 1**

**3 FEBRUARY 2003**

**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: SFC (TSgt Kenneth Ingles)

Certified by: SF (Mr. James E. Moree)

Pages: 4

Distribution: F

---

The OPR for this supplement is SFC (TSgt Kenneth Ingles). This publication supplements AFI 31-501, *Personnel Security Program*, 1 August 2000. This supplement applies to all Air Force Space Command (AFSPC) personnel and tenant units on AFSPC installations. This supplement provides a baseline requirement for managing the Personnel Security Program. Deviations to this supplement must first be approved by the OPR prior to implementation. Send comments and suggested improvements on AF Form 87, Recommendation for Change of Publication, to HQ AFSPC/SFC, 150 Vandenberg Street, Suite 1105, Peterson AFB, CO 80914-4560. Provide copies of base supplements to AFI 31-501 and this AFSPC supplement to HQ AFSPC/SFC. Does not apply to AFRC/ANG unless tenants units on AFSPC installations

1.1.2. All waiver requests must also be forwarded through HQ AFSPC/SFC.

3.1. **Authority to Designate Sensitive Positions.** Commanders are responsible for determining whether or not their personnel need a specific personnel security investigation and/or access. NEVER submit an investigation because of personal reason. And NEVER, submit an investigation on personnel who are retiring or separating within 12 months.

3.1.1. (Added) Expired Investigation: Forward a Security Information File (SIF) option letter to the subject's commander. If the commander is unwilling to establish a SIF and the Installation Security Program Manager (ISPM) does not concur, forward SIF option letter to the installation commander.

3.1.2. (Added) Security managers are responsible for ensuring their unit personnel submit their PSIs accurately and on-time.

3.11.1.2. If the Electronic Personnel Security Questionnaire (EPSQ) or SF Form 86, **Questions for National Security Positions**, is unavailable, the member will complete another for the commander's review.

3.11.1.4. If phone verification is used for the receipt a Memo For Record will be accomplished and attached to the AF Form 2583, **Request for Personnel Security Action**.

3.11.2.1. If the EPSQ or SF Form 86 is unavailable, the member will complete another EPSQ or SF86 for the commander's review.

3.11.2.4. If phone verification is used for the receipt, a Memo For Record will be accomplished and attached to the AF Form 2583.

3.11.4. Utilize the AF Form 2583 and Joint Personnel Adjudication System (JPAS) to document all interim security clearance actions.

5.1.1.2. (Added) Security Managers will:

5.1.1.2.1. (Added) Manage the unit's Personnel Security Program within their unit or staff agency.

5.1.1.2.2. (Added) Develop and update a unit security operating instruction. Refer to the ISPM for minimal requirements.

5.1.1.2.3. (Added) Advise their commander or staff agency chief on personnel security issues pertaining to the unit or staff agency.

5.1.1.2.4. (Added) Attend ISPM hosted security manager meetings.

5.1.1.2.5. (Added) Update and remind personnel of personnel security policies and procedures.

5.1.1.2.6. (Added) Monitor all Personnel Security Investigations (PSI) for their respective unit through JPAS. Provide, on a weekly basis, the status of each submitted investigation to the ISPM or designative representative.

5.1.1.2.7. (Added) Review all PSI for errors, before they are submitted to the ISPM or designated representatives.

5.1.1.2.8. (Added) Develop and conduct a training plan tailored to the unit's personnel security issues. Training must be documented and conducted at least annually.

5.1.2. (Added) ISPM and/or the designated representative will forward every Friday, to HQ AFSPC/SFC the status of all PSI that have been submitted. Status information will be sent in an excel document utilizing the following format:

5.1.2.1. (Added) Column 1: LAST NAME, First Name, Middle Initial.

5.1.2.2. (Added) Column 2: Current rank.

5.1.2.3. (Added) Column 3: Social security number (XXX-XX-XXXX).

5.1.2.4. (Added) Column 4: Numbered Air Force (14, 20, SMC).

5.1.2.5. (Added) Column 5: Wing (21 SW, 30 SW, 45 SW, 50 SW, 90 SW, 91 SW, 341 SW, 460 ABW, or SMC).

5.1.2.6. (Added) Column 6: Unit assigned too.

5.1.2.7. (Added) Column 7: Office assigned too.

5.1.2.8. (Added) Column 8: Current AFSC.

5.1.2.9. (Added) Column 9: Date sent to DSS (If applicable) in DD-MMM-YY format.

5.1.2.10. (Added) Column 10: Date sent to OPM (If applicable) in DD-MMM-YY format.

5.1.2.11. (Added) Column 11: Date investigation was open in DD-MMM-YY format.

- 5.1.2.12. (Added) Column 12: Date investigation was closed at AFCAF in DD-MMM-YY format.
- 5.1.2.13. (Added) Column 13: Type of investigation submitted (“T” - Top Secret, “S”- Secret, and “TS-SCI”- Top Secret SCI).
- 5.1.2.14. (Added) Column 14: Put an “X” for initial investigation.
- 5.1.2.15. (Added) Column 15: Put an “X” for periodic reinvestigation.
- 5.1.2.16. (Added) Column 16: Put the appropriate PRP code (If applicable). Put an “X” if it’s a PRP PR investigation.
- 5.2.2. Units will forward all deletion and additions for authorized requesters to HQ AFSPC/SFC. HQ AFSPC/SFC will manage and submit all lists to Air Force Central Adjudication Facility (AFCAF).
- 5.6.1. Investigation must be submitted 6 months prior to an investigation expiring. It is the security managers’ responsibility to ensure unit personnel are notified 8 months prior to an investigation expiring.
- 5.6.2. The security manager will review all PSI packages to ensure packages are error free. Security managers must not rely on the EPSQ program to validate packages.
- 7.1.2.5. (Added) Before granting access to classified information the following must be accomplished:
- 7.1.2.5.1. (Added) Appropriate investigation has been completed and adjudicated by the AFCAF.
- 7.1.2.5.2. (Added) Standard Form 312, **Non Disclosure Agreement**, has been signed. If the SF 312 cannot be verified, a new SF 312 will be accomplished and entered into JPAS.
- 7.1.2.5.3. (Added) The commander has granted access (indoctrinated). Security Managers will verify through JPAS that indoctrination authority has been given. Granting access to classified is based on access authority, not the individual’s eligibility status.
- 7.1.2.6. (Added) The commander grants access to classified information by the security manager "Indoctrinating" the member through JPAS.
- 7.4.2.5. Before access to JPAS is granted, the following must be accomplished:
- 7.4.2.5.1. (Added) Appropriate security background investigation. Account Managers (Level 5) and security managers (Level 6) must have a National Agency Check & Credit Check (NACLC) or Access National Agency Check with Inquiries (ANACI) investigation.
- 7.4.2.5.2. (Added) Completion and passing the Account Manager and/or User JPAS computerized training course provided by HQ AFSPC/SFC and/or JPAS web page. Additional training will also be provided by the ISPM during initial security managers training.
- 7.4.2.5.3. (Added) Level 5 access will only be given to personnel working in, or associated with the Information, Personnel, and/or Industrial Security Programs.
- 7.4.2.5.4. (Added) Level 6 access will only be given to personnel performing duties as Security Manager and/or Personnel Reliability Program (PRP) monitor. All others positions must be approved by the ISPM and/or the MAJCOM account managers.
- 7.4.2.5.5. (Added) Access will not be given to contractors.
- 7.4.2.6. Requesting JPAS access:

7.4.2.6.1. Security managers will complete their Access Request Letter (ARL) for Level 6 access and forward to their ISPM. The ISPM will verify the member meets the requirements, sign, and file.

7.4.2.6.2. ISPM will complete and forward their ARL for Level 5/Account Manager access to HQ AFSPC/SFC by fax or mail. HQ AFSPC/SFC will verify the member meets the requirements, sign, and file.

7.4.2.8. JPAS Management.

7.4.2.8.1. (Added) The ISPM will manage their bases JPAS account (Level 5, 6, and 7).

7.4.2.8.2. (Added) Accounts will be reviewed annually by the ISPM.

7.4.2.8.3. (Added) Personnel found abusing their JPAS access will be have their access removed. The installation commander must approve request for reinstatement.

7.4.2.8.4. (Added) Only UNCLASSIFIED information will be entered into JPAS.

7.4.2.8.5. (Added) All problems associated with JPAS will be reported to the ISPM and/or designated representatives. If the issue cannot be resolved locally, the ISPM and/or designated representatives will notify the MAJCOM account managers. Under no circumstances are Level 6 and 7 personnel permitted to contact JPAS and report access problems.

7.4.2.8.6. (Added) Erroneous data (i.e. wrong date of birth, place of birth, rank, etc.) will be reported through the base MPF. Reporting erroneous date through JPAS will not correct the data.

7.4.2.8.7. (Added) All accounts discovered inactive for 3 months will be deleted.

10.3. **Safeguarding Procedures.** At a minimum, all PSI's must be stored in a locking filing cabinet and/or locked room.

MICHAEL W. HAZEN, Col, USAF  
Director of Security Forces