

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



**AIR FORCE INSTRUCTION31-
501_AFSPCSUP**

**AIR FORCE SPACE COMMAND
Supplement**

6 JUNE 2012

Certified Current on 9 May 2013
Security

**PERSONNEL SECURITY PROGRAM
MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publication and forms are available on the e-publishing website at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFSPC/IP

Certified by: AFSPC/IP
(Mr. James M. Krall)

Supersedes: AFI 31-501_AFSPCSUP, 16
June 2008

Pages: 9

This supplement implements and extends the guidance of AFI 31-501, *Personnel Security Program Management*, 27 January 2005. This supplement describes AFSPC's procedures for use in conjunction with the basic AFI. This supplement applies to all AFSPC personnel and tenant units on AFSPC installations. This supplement applies to Air Force Reserve Command units tenant on AFSPC installations and participating under program oversight. This supplement does not apply to Air National Guard units. This supplement provides a baseline requirement for managing the Personnel Security Program. Deviations to this supplement must be approved by the Office of Primary Responsibility (OPR) prior to implementation. Refer recommended changes and questions about this publication to the OPR using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional's chain of command. Provide copies of base supplements to AFI 31-501 and this supplement to HQ AFSPC/IP. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Major changes include removal of instructions for the submission of waivers through IP channels, instructions clarifying when Access National Agency Check with Written Inquiries and Credit Check submissions are required for new civilian personnel, requirement to submit periodic reinvestigations on personnel occupying non-critical positions who do not access classified information, requirement for the Servicing Security Activity (SSA) to review unit personnel security programs during information security program reviews, instructions to use www.sss.gov to obtain selective service numbers, specifications of what constitutes a local files check, and the requirement that the local files check not exceed 30 days from the date of first signature. In addition, instructions for the delivery of Statement of Reasons were modified (paragraph 8.6.1.1.). Further revisions are made for clarity and currency.

2.4. Types and Scope of Personnel Security Investigations. Electronic Questionnaire for Investigation Processing (e-QIP) replaces Electronic Personnel Security Questionnaire (EPSQ) as used throughout the basic AFI.

3.11. **Interim Security Clearances.** Security managers will coordinate interim clearances with the SSA prior to the commander granting the interim clearance. The SSA will ensure all interim security clearance requirements have been met and any potentially derogatory information is identified for the commander's review. The SSA may make recommendations to the subject's commander about whether an interim clearance should be granted. The subject's commander will determine what is considered to be "favorable" when determining whether to grant an interim security clearance. The commander will use the sample memorandum at Attachment 27 (Added) or similar memorandum to grant interim clearances. The security manager will maintain the signed memorandum, the AF Form 2583, *Request for Personnel Security Action*, and all coordination for the life of the interim clearance. When interim security clearances are terminated for cause, an AF Form 2587, *Security Termination Statement*, must be accomplished.

3.11.1.3. If a copy of the submitted personnel security questionnaire (PSQ) is not available for review, the subject will complete a hardcopy Standard Form (SF) 86, *Questionnaire for National Security Positions*, for the commander's review.

3.11.3. The SSA will maintain a memorandum for record (MFR) documenting NAC results provided by the Air Force Central Adjudication Facility (AFCAF) until the investigation is adjudicated. Provide a copy of the MFR to the individual's security manager.

3.11.4.1. If a copy of the submitted PSQ is not available for review, the subject will complete a hardcopy SF 86 for the commander's review.

3.14.2.1. **(Added)** Commanders will ensure consultants working for their organization who require access to classified information prepare and submit the appropriate security clearance application to the SSA through the unit security manager. The interim security clearance provisions in paragraph 3.11. apply.

3.15.1. **(Added)** Coordinate one time access with the SSA. The approval authority will document access on AF Form 2583. The unit security manager will maintain the AF

Form 2583 until access is no longer required. Execute AF Form 2587 upon termination of access.

3.30. **(Added)** Contractor Suitability Determinations. Unit commanders will make suitability determinations for contractors assigned to their unit who require a favorable background investigation for contract performance. All unfavorable determinations must be approved by the installation commander. The installation commander's decision is final.

3.30.1. **(Added)** The installation commander will make suitability determinations for contractors assigned to an on-base cleared facility requiring a favorable background investigation. This authority may be delegated to another government activity.

5.1.1. Security managers will also support contractors requiring favorable background investigations for contract performance.

5.2.2. SSAs will forward all additions (include name, rank, Social Security number, DSN number, and office symbol) and deletions for authorized callers to HQ AFSPC/IP. SSAs will annotate on authorized caller addition letters those personnel who require Central Adjudication Security Personnel Repository (CASPR) accounts. HQ AFSPC/IP will provide a consolidated authorized caller list for the command to the AFCAF.

5.7. **Dual Citizenship.** Interim security clearances will not be granted to dual citizens until the provisions of the basic instruction have been met.

7.1.2.1. The SSA will forward the change request to the servicing manpower office.

7.4.2.5. Contractors providing collateral security support may be given level 7 or level 10 Joint Personnel Adjudication System (JPAS) accounts. Access to levels 4, 5, or 6 will not be granted to contractors.

7.4.2.6.5. SSAs submit access request forms for level 5/account manager access to HQ AFSPC/IP for approval. Geographically separated units (GSUs) will route their requests to their parent wing.

7.6.5. Additional/new/upgrade SSBI requests will be routed through the wing commander to the NAF/CC or SMC/CC. AFSPC/CV is the approval authority for headquarters elements. All requests must include detailed justification to ensure only those positions having a valid need-to-know are upgraded. Use the sample memorandum at **Attachment 28 (Added)**. SSAs will maintain a copy of the approval until the investigation is adjudicated.

7.9.3. Collateral level (levels 4, 5, 6, 7, and 10) account management access is restricted to HQ AFSPC/IP and SSA staff members. The SSA will designate account managers to HQ AFSPC/IP. SSAs will maintain a signed access request form for each user for the life of the account and will conduct an annual review of all subordinate accounts to ensure all accounts are valid. JPAS users found abusing their JPAS access (i.e., account sharing, use for other than government purposes, failing to protect information in accordance with the Privacy Act of 1974, or any other actions deemed inappropriate) will have their access removed. The installation commander must approve request for reinstatement.

7.9.5.3.1. **(Added)** Level 4 access is limited to HQ AFSPC/IP staff.

7.9.5.4.1. **(Added)** Level 5 access is limited to SSA staff.

7.9.5.5.1. **(Added)** Level 6 accounts are restricted to appointed unit security managers and Civilian Personnel staff (for e-QIP purposes only). Installation Personnel Reliability Program (PRP) managers may be given level 6 accounts as necessary to perform their duties. Other personnel who justify a need to the SSA for a JPAS account may be given a level 7 or 10 account.

7.9.6. **(Added)** Security managers must maintain a JPAS account. Security managers will manage JPAS for their unit by performing the following functions:

7.9.6.1. **(Added)** Maintaining the PSM Net by in-processing and out-processing all unit personnel. Security managers will “own” all permanently assigned personnel, and they will “service” all contractors assigned to integrated visitor groups supporting their unit.

7.9.6.2. **(Added)** Recording and removing applicable accesses using the “indoctrinate” link. Personnel will be indoctrinated for the level of access required for the position.

7.9.6.3. **(Added)** Annotating SF 312, *Classified Information Non-Disclosure Agreement*, and verbal attestation dates using the “indoctrinate” link.

7.9.6.4. **(Added)** Sending, receiving, and managing visit notifications as required.

7.9.6.5. **(Added)** Monitoring and acting on system notifications.

7.9.7. **(Added)** SSAs will maintain the installation PSM Net by “servicing” assigned personnel.

8.2.1.3.1.2. SSAs will recommend establishing a security information file (SIF) with access suspension for personnel who fail to submit their periodic reinvestigation on time. Top Secret PRs are considered to be overdue 5 years and 1 day after the previous investigation closed. Secret PRs are considered to be overdue 10 years and 1 day after the previous investigation closed.

8.2.1.4.1. **(Added)** If access is suspended, an AF Form 2587 must be accomplished and included in the SIF.

8.2.2.1.1. **(Added)** A personnel security representative from the SSA will attend the installation “Cops and Robbers” (or equivalent) meeting. The representative will take appropriate personnel security action (see paragraph 8.2.2.1.2.) based on information discovered during the meeting.

8.2.2.1.2. **(Added)** When the SSA becomes aware of potentially derogatory information, the SSA will use the sample memorandum at Attachment 11 of the basic instruction or a similar memorandum to notify the individual’s commander to consider SIF establishment. If the individual is Sensitive Compartmented Information (SCI)-indoctrinated, notify the servicing Special Security Office (SSO), who will in turn notify the individual’s commander.

8.6.1.1. **(Added)** Statements of reason (SOR) are sent to the subject’s commander through the SSA. Upon receipt, the SSA will deliver the SOR to the subject’s commander and will thoroughly explain the SOR. This cannot be delegated.

8.6.2. Submit appeals through the SSA.

8.6.3.1. **(Added)** Since SORs are sensitive in nature, careful consideration must be given in the selection of the designated point of contact (POC). The POC must be an individual responsible for handling sensitive personnel issues, such as first sergeants, supervisors, deputy commanders/directors, etc.

8.6.4. Submit response through the SSA. The SSA will provide any assistance necessary to the designated POC and the subject in responding to the SOR. The SSA will update the "SOR Update" screen in JPAS with each action for tracking purposes.

8.7. **Security Clearance Reinstatement.** Submit requests through the SSA.

10.4. **(Added) File Copy Personnel Security Questionnaires (PSQ).** File copy PSQs must remain under the control of the authorized requester. If it becomes necessary for files (hard copy or electronic) to be removed from the authorized requester's file plan for inspections, etc., each file will be receipted and accounted for. Copies of files will not be made for convenience purposes. Personnel security investigation (PSI) subjects are encouraged to maintain a personal copy of their completed PSQ. Security managers will not maintain PSQ copies for unit personnel.

JAMES E. MOREE JR., GS-15, DAF
Director of Information Protection

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFMAN 33-363, *Management of Records*, 1 March 2008

Prescribed Forms

This supplement does not prescribe any forms.

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 2583, *Request for Personnel Security Action*

AF Form 2587, *Security Termination Statement*

SF 86, *Questionnaire for National Security Positions*

SF 312, *Classified Information Non-Disclosure Agreement*

Attachment 2

REQUEST PROCEDURES

A2.2. 2.2. E-QIP will be utilized to submit PSI requests.

A2.2.2.5. Utilize instructions in OPM Federal Investigative Services INV 15 for submission requirements.

A2.2.2.9. Electronic suspense copies may be maintained on a secure server in an approved electronic file plan. Access will be limited to SSA staff members.

A2.7.2.1. **(Added)** Security managers will request e-QIP initiation so the SSA can initiate the reinvestigation 60 days prior to the anniversary date of the current investigation. **EXCEPTION:** For deployed members, e-QIP will be initiated immediately upon their return to home station duty.

A2.7.2.1.1. **(Added)** Subjects will complete their e-QIP within 30 days of initiation. If the subject fails to complete their e-QIP within the allotted time, the individual's commander must request re-initiation of the e-QIP. If the subject fails to complete their e-QIP within 30 days of re-initiation, the commander will consider establishing a SIF.

A2.7.3.1. **(Added)** Security managers will request e-QIP initiation so the SAA can initiate the reinvestigation 60 days prior to the anniversary date of the current investigation. **EXCEPTION:** For deployed members, e-QIP will be initiated immediately upon their return to home station duty.

A2.7.3.1.1. **(Added)** Subjects will complete their e-QIP within 30 days of initiation. If the subject fails to complete their e-QIP within the allotted time, the individual's commander must request re-initiation of the e-QIP. If the subject fails to complete their e-QIP within 30 days of re-initiation, the commander will consider establishing a SIF.

Attachment 27 (Added)**SAMPLE INTERIM SECURITY CLEARANCE APPROVAL LETTER****DEPARTMENT OF THE AIR FORCE****AIR FORCE UNIT HEADING**

MEMORANDUM FOR RECORD

FROM: UNIT COMMANDER

SUBJECT: Interim Clearance, Amn John Doe, SSN:

1. I have favorably reviewed subject's SF 86 and AF Form 2583 and hereby grant an interim Secret/Top Secret clearance.
2. Direct any questions to the unit security manager.

Commander's Signature Block

Attachment 28 (Added)

SAMPLE POSITION CODE 5 UPGRADE REQUEST MEMORANDUM

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR NAF/CC or SMC/CC

FROM: (Organizational Commander)

SUBJECT: Position Code 5 Upgrade Request

1. Request NAF/CC (or SMC/CC) approval for an upgraded Single Scope Background Investigation (SSBI) requirement of the manning position(s) identified below:
 - a. (Unit, organization, and office symbol for the position)
 - b. (Unit manning document position number)
 - c. (Position Air Force Specialty Code (AFSC) or civilian career field series number)
 - d. (Position rank/grade)
 - e. (Position Title)
2. Justification. (Provide complete justification why the new or current position should be changed to an SSBI requirement, to include specific duties and responsibilities warranting routine and regular access to Top Secret information. State whether SCI access is required.)
3. Mission Impact. (Provide complete assessment on the impact to the mission if this request is not approved.)
4. POC for this request is (grade, name, organization/office symbol, and DSN).

Commander's Signature Block