

**BY ORDER OF THE COMMANDER
AIR FORCE GLOBAL STRIKE COMMAND**

AIR FORCE INSTRUCTION 31-501



**AIR FORCE GLOBAL STRIKE COMMAND
SUPPLEMENT**

20 AUGUST 2010

Information Protection (IP)

PERSONNEL SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at <http://www.e-Publishing.af.mil/> for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFGSC/IP

Certified by: HQ AFGSC/IP
(Mr. David W. Sweeney)
Pages: 9

This supplement implements and extends the guidance of AFI 31-501, *Personnel Security Program Management*, 27 January 2005. This supplement describes Air Force Global Strike Command (AFGSC) procedures for use in conjunction with the basic Air Force Instruction (AFI). This supplement applies to all AFGSC personnel and tenant units on AFGSC installations. 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 IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional chain of command. Provide copies of base supplements to AFI 31-501 and this supplement to Headquarters Air Force Global Strike Command/Information Protection (HQ AFGSC/IP). This supplement applies to Air National Guard and Air Force Reserve units tenant on AFGSC installations and participating under program oversight. This instruction requires collecting and maintaining information protected by the *Privacy Act of 1974* authorized by 10 U.S.C. 8013, Secretary of the Air Force and E.O. 9397 (SSN). System of Records notice F031 AF SP M, Personnel Security Access Records applies. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims/>. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

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

2.4.3. National Agency Check with Inquiries (NACI) is now the baseline investigation. All AF positions (civilian/contractor) that previously required the initiation or completion of a National Agency Check (NAC) will now require a NACI or higher investigation. This includes personnel who require unescorted entry into sensitive areas, non-appropriated fund employees in public trust positions, contract guards, personnel assigned to IT-II or IT III positions and volunteers.

2.4.5. Access National Agency Check with Written Inquiries and Credit Check (ANACI) is required for all civilian employees assigned to noncritical sensitive positions. National Agency Check, Local Agency Check and Credit Check (NACLIC), and National Agency Check (NAC) are not sufficient in scope for personnel assigned to these positions. **EXCEPTION:** Single Scope Background Investigations (SSBI) are sufficient in scope for civilians assigned to noncritical sensitive positions, provided there has been no break in service greater than 24-months.

3.2. Within AFGSC, the installation IP Office submits all Personnel Security Investigation (PSI) requests.

3.5. Periodic Reinvestigations (PRs) for Critical Sensitive and Noncritical Sensitive Positions. PRs are required for all civilian employees in noncritical sensitive and critical sensitive positions regardless of classified information access requirements.

3.7. Mobilization of DoD Civilian Retirees. Send waiver requests for investigative requirements to HQ AFGSC/IP.

3.9. Mobilization of Military Retirees. Send waiver requests for investigative requirements to HQ AFGSC/IP.

3.11. Interim Security Clearances. Security managers will coordinate interim clearances with the servicing Wing Information Protection (IP) office prior to the commander granting the interim clearance. The Wing IP will ensure all interim security clearance requirements have been met and any potentially derogatory information is identified for the commander's review. The Wing IP may make recommendations to the subject's commander concerning eligibility. The subject's commander will determine what is considered to be "favorable" when determining whether to grant an interim security clearance. Document interim security clearances by using AF IMT 2583, **Request for Personnel Security Action**. Unit commanders sign Item 26 when granting the interim security clearance. The SSA and Security managers will keep a suspense copy of the AF IMT 2583 until the clearance eligibility is updated in Joint Personnel Adjudication System (JPAS). Annotate interim clearances in the Joint Clearance and Access Verification System (JCAVS) once the AF IMT 2583 is signed by the commander. When interim security clearances are terminated for cause, an AF IMT 2587, **Security Termination Statement**, must be accomplished.

3.11.3. The Wing IP 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.

3.11.6.1. Former military members with a break in service of 2 years or less and SSBI within 5 years do not have to resubmit an SSBI for critical sensitive positions. Periodic Reinvestigations will be submitted for SSBI over 5 years old. Former military members and current reserve and guard personnel occupying noncritical sensitive positions must submit an Access National Agency Check with Written Inquiries and Credit Check (ANACI). Members occupying noncritical sensitive positions with a break in service of 2 years or less and SSBI within 10 years do not have to submit an ANACI until the SSBI reaches the 10 year mark.

3.12.1. Initial Limited Access Authorization (LAA). Send LAA requests to HQ AFGSC/IP. If approved, SSBI will be sent to OPM for processing instead of DSS.

3.15. One Time Access. Document one time access by using AF IMT 2583. Approving authorities sign Item 26 when granting access. The sponsoring activity security manager will maintain the AF IMT 2583 until the access is no longer needed. Complete an AF Form 2587, **Security Termination Statement**, when access is terminated. Document actions in JCAVS when applicable.

3.16. Processing Requests for Access by Retired General Officers or Civilian Equivalents. Document retired general officer access by using AF IMT 2583. Approving authorities sign Item 26 when granting access. The sponsoring activity security manager will maintain the AF IMT 2583 until the access is no longer needed. Complete an AF IMT 2587 when access is terminated. Document actions in JPAS when applicable.

3.24.7. The MAJCOM Vice Commander (HQ AFGSC/CV) is delegated the authority to hear appeals of denials or withdrawals for unescorted entry into restricted areas. Send appeals of denials or withdrawals of unescorted entry to HQ AFGSC/IP for processing.

3.24.10. The Wing IP submits the applicable background investigation to OPM for contractor personnel requiring unescorted entry to restricted areas. This only applies to contractors who do not require access to classified information.

3.27.3. Commanders may recommend to the Wing Certifying Authority (WCA) that interim Automated Information System (AIS) access be granted. WCAs may waive on a case by case basis the investigative requirements for access to AIS pending completion of a favorable NACI, NACIC, ANACI, or SSBI after favorable review of the completed personnel security questionnaire for the investigation. WCAs will confirm interim AIS access requirements are met prior to access.

3.27.3.7.2. The Wing IP submits the applicable background investigation to OPM for contractor personnel requiring access to unclassified AIS. This only applies to contractors who do not require access to classified information.

3.29. Explosive Ordnance Disposal (EOD). Members assigned to EOD positions, Air Force Specialty Code (AFSC) 3E8, require SSBIs and PRs on a five year recurring basis (HQAF/XOS-FI memo dated 11 Feb 05).

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 forwarded to the installation commander for review and final unfavorable decision. 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 provide personnel security support to integrated visitor group contractors occupying positions of trust that require trustworthiness and reliability determinations. Security managers will submit the applicable background investigation to the Wing IP for processing to OPM. This only applies to contractors who do not require access to classified information.

5.2.1. Wing Information Protection (Wing/IP) offices are designated as the authorized requester of investigations on AFGSC installations. Send requests for additional authorized requester codes to HQ AFGSC/IP.

5.2.2. Wing IP will forward all additions (include name, rank, Social Security number, DSN number, and office symbol) and deletions for authorized callers to HQ AFGSC/IP. HQ AFGSC/IP will provide the authorized caller list to the AFCAF.

5.5.1. Personnel Reliability Program (PRP). The provisions of this paragraph only apply when the member is "C" coded and cannot be interim certified or put to work for a valid reason, i.e., a final investigation is required, issues have been identified that would prevent an interim certification.

7.1.2.1. The Wing IP will forward the change request to AFGSC/IP and the servicing manpower office .

7.2.1.3. Reviews will be documented in writing and signed by the commander. Security managers will maintain the signed documentation until the next annual review is conducted.

7.4.2.6.5. Wing IP will submit access request forms for level 5/account manager access to HQ AFGSC/IP for approval.

7.4.2.6.5. Access request forms for levels 6, 7, and 10 access will be submitted to The Wing IP for approval.

7.5. Investigative Requirements for Air Force Deployments, Operational or Contractual Exigencies. Home station commanders will coordinate this action with deployed commanders before granting interim Top Secret access. Document interim Top Secret access by using AF IMT 2583. Commanders sign Item 26 when granting the interim access. The deployed member will maintain the original AF IMT 2583 for use at the deployed location and the home station servicing security manager will maintain a copy of the AF IMT 2583. Access will be discontinued upon return to home station by executing an AF IMT 2587.

7.6.5. Additional/new/upgrade SSBI requests will be routed through the Wing IP. Commanders will request approval through manpower channels to HQ AFGSC/CC. HQ AFGSC/CC 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). Wing IP 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 AFGSC/IP and Wing IP staff members. The Wing IP will designate account managers to HQ AFGSC/IP. Wing IPs 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 AFGSC/IP staff.

7.9.5.4.1. (Added). Level 5 access is limited to Wing IP staff.

7.9.5.5.1. (Added). Additional level 6 access is approved by Wing Chief, Information Protection.

7.9.6. (Added). Security managers must maintain a JPAS account. Security managers will manage JPAS within their organizations 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.

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.

7.9.6.6. (Added). Maintaining a copy JCAVS Eligibility and Access Report current within the last 30 days.

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

8.2.1.7. Once all pertinent information is obtained to close the SIF, the commander will request closure of the SIF in writing to the AFCAF through the Wing IP. The memo will include a recommendation whether to grant, reinstate, deny, or revoke the individual's security clearance.

8.2.2.1.1. (Added). When the Wing IP becomes aware of potentially derogatory information, the Wing IP 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 SCI-indoctrinated, notify the servicing Special Security Office (SSO), who will in turn notify the individual's commander.

8.5.2. SIFs will not be created for civilian employees in nonsensitive positions.

8.6.2. Submit appeals through the Wing IP.

8.6.4. Submit response through the Wing IP. The Wing IP will provide any assistance necessary to the designated POC and the subject in responding to the Statement of Reason (SOR). The Wing IP will update the "SOR Update" screen in JPAS with each action for tracking purposes.

8.7. Security Clearance Reinstatement. Submit requests through the Wing IP.

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.

11.1.4.1. (Added). Wing IP will review units' personnel security programs during information security program reviews.

DOUGLAS C. LITTLE, GS-14, USAF
Director, Information Protection

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

AFI 31-501, <http://www.e-publishing.af.mil/pubfiles/af/31/afi31-501/afi31-501.pdf>, *Personnel Security Program Management*, 27 January 2005 Air Force Records Information Management System, <https://afirms.amc.af.mil/rds/index.cfm>, *Air Force Records Disposition Schedule*

Abbreviations and Acronyms

AFCAF – Air Force Central Adjudication Facility

AFRC – Air Force Reserve Command

ANACI - National Agency Check with Written Inquiries and Credit Check

ANG – Air National Guard

DoD – Department of Defense

EOD – Explosive Ordnance Disposal

HQ AFGSC/IP – AFGSC Information Protection Directorate

JPAS – Joint Personnel Adjudication System

NACI - National Agency Check with Inquiries

NACLIC - National Agency Check, Local Agency Checks and Credit Check

PSM NET – Personnel Security Management Network

RDS – Records Disposition Schedule

SSA – Servicing Security Activity

SSBI – Single Scope Background Investigation

Terms

Joint Personnel Adjudication System (JPAS)—The DoD system of records for personnel security and access information.

Office of Personnel Management (OPM)—The DoD Authorized Personnel Security Investigation Provider.

Attachment 2

REQUEST PROCEDURES

A2.2.2.2. e-QIP by design will be utilized to submit Personnel Security Investigation (PSI) requests.

A2.2.2.5. Utilize Office of Personnel Management (OPM) instructions for submission requirements.

A2.2.2.9. Authorized requesters will maintain a suspense copy of PSIs initiated on their installation along with all other applicable information until the clearance eligibility is updated in the JPAS. Authorized requesters will also maintain PSIs received from other installations until clearance eligibility is updated in JPAS. Electronic suspense copies may be maintained on a secure server in an approved electronic file plan. Access will be limited to Wing IP staff members.

A2.2.2.10. Security managers and authorized requesters will check JPAS weekly to monitor the status of investigations and clearance eligibility.

A2.2.3.2.3. Obtain selective service number information at www.sss.gov.

A2.6. AF IMT 2583 will be used to annotate local file check, which will consist of a check of local personnel files, a check of medical files (if applicable), and a check of the Security Forces Information Management System (SFMIS). The National Crime Information Center (NCIC) is not authorized to be utilized for local file checks. Security managers will maintain the completed AF IMT 2583 until the clearance eligibility is updated in JPAS. Authorized requesters will maintain a copy of the AF IMT 2583 until the clearance eligibility is updated in JPAS.

A2.7.2.1. (Added). Security managers will request e-QIP initiation at the 9.5 year mark. 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.

A2.7.3.1. (Added). Security managers will request e-QIP initiation at the 4.5 year mark. 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.

Attachment 28 (Added)

SAMPLE POSITION CODE 5 UPGRADE REQUEST MEMORANDUM

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR HQ AFGSC/CC

FROM: (Organizational Commander)

SUBJECT: Position Code 5 Upgrade Request

1. Request HQ AFGSC/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