



Security

**PERSONNEL SECURITY
PROGRAM MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications 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: 1 SFS/S-5
Supersedes AFI31-501_HURLBURTFIELDSUP1,
1 December 2003

Certified by: 1 SFS/CC (Major Marc A. Sheie)
Pages: 10

This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-501, *Personnel Security Program Management*, 27 January 2005. This supplement establishes procedures for implementing Air Force Policy Directive (AFPD) 31-5, Personnel Security, and Air Force Instruction (AFI) 31-501, Personnel Security Program Management. It applies to all personnel assigned to Hurlburt Field unless stated otherwise in the installation support agreement.

SUMMARY OF CHANGES

This change implements the requirements of AFI 31-501, 27 January 2005, and to identify changes in local procedures, and realigns chapter and paragraph references.

1.1.2. Send waivers, inquiries and recommendations for changes to AFI 31-501 and Hurlburt Field Supplements to 1 SFS/S-5. Coordinate unit operating instructions (OIs) with 1 SFS/S-5.

1.1.3. (Added) The servicing security activity (SSA) at Hurlburt is 1 SFS/S-5.

3.1. **Authority to Designate Sensitive Positions.** Commanders are responsible for determining whether their personnel require specific personnel security investigations and/or access. NEVER submit a personnel security investigation (PSI) because of personal reasons. And NEVER, submit an investigation on personnel who are retiring or separating within 12 months. Refer to the mandatory single scope background investigation (SSBI) listing, Joint Personnel Adjudication System summary sheet or unit manning document (UMD) when determining position sensitivity (PS) codes.

3.6. **Pre-Employment Waivers.** The civilian personnel flight (CPF) 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. Appointment prior to completion of the investigation is necessary to accomplish fill action in support of national security. A pre-employment waiver does not authorize the individual access to classified information, automated information system

access (AIS) or a restricted area badge. The individual must have a security clearance for access to classified information or at least a favorable national agency check (NAC) investigation for access to AIS and unescorted entry to restricted areas. If member had more than a 2-year break in service, resubmit them for a new investigation. Prior military members hired as civilian government employees into non-critical sensitive positions are required to submit an initial access national agency check with inquiries (ANACI) investigation. Members with secret access while in military status will retain that access pending the outcome of the initial ANACI investigation. If the prior investigation was a NAC, entrance national agency check (ENTNAC) or national agency check with inquiries (NACI), fingerprints are required.

3.7. **Mobilization of DoD Civilian Retirees.** Use AF Form 2583 to submit request to SSA.

3.8. **Military Appointment, Enlistment, and Induction.** Use AF Form 2583 to submit request to SSA.

3.11. **Interim Security Clearances.** Use AF Form 2583 to submit requests for interim security clearances to SSA. Commanders may grant interim security clearances, through 1 SFS/S-5, 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 and AFI 31-501, paragraph 3.11. have been met. Interim security clearances will not be granted if the current investigation is closed and in adjudication. Approved interims will be entered into joint personnel adjudication system (JPAS) by 1 SFS/S-5. Interim clearances may be revoked at any time based on unfavorable information identified in the course of the investigation. Interim clearances should be limited 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 1 SFS/S-5 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 (NACLIC), or Access National Agency Check with Written Inquiries and Credit Check (ANACI) has been completed with no break in service over 2 years.

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 Questionnaire Investigations Processing (e-QIP), SF 86, UPRG, *Questionnaire for National Security Positions*), and local files. Commander signs block 13 of AF 2583 requesting the interim clearance. Remarks section of AF Form 2583 must include a statement that personnel records have been reviewed, and derogatory information does/does not exist.

3.11.1.3.1. (Added) In e-QIP, the investigation is submitted after the electronic finger prints are sent (if required), authorization release forms are sent and the personnel security investigation (PSI) is reviewed/approved and submitted to Office of Personnel Management (OPM). All investigations must have been submitted by an authorized requester to the investigative agency provider.

3.11.4. Interim secret clearances must be based on all of the following:

3.11.4.1. Unit commander or staff agency chief must conduct a favorable review of the individual's SF 86, and local files. Commander signs block 13 of AF 2583 requesting the interim clearance.

3.11.4.2. 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.

3.11.4.3. The 1 SFS/S-5 must verify a NACLIC or ANACI has been submitted by an authorized requester to an investigative agency provider.

3.11.4.4. (Added) Submission verification must be made through JPAS. See **3.11.1.3.1. (Added)** for PSI submission requirements.

3.11.5. When an individual has been granted an interim clearance at a previous location and it is recorded in JPAS, the gaining unit commander may review the individual's SF 86 and local PIF to decide whether to honor the previously granted interim. Document interim clearances in writing if JPAS is unavailable. Notify 1 SFS/S-5 of any changes in interim clearance eligibility status.

3.14.2. Host organization using consultants are responsible for submission of clearance applications.

3.15. **One Time Access.** Request for one time access must be submitted to SSA using AF Form 2583. Host organization security manager is responsible for conducting files review, same as for interim top secret, submitting request and maintaining a file until access is no longer needed. Approving authorities at Hurlburt are 1 SOW/CC, 1 SOW/CV AFSOC/CC or AFSOC/CV Upon approval, 1 SFS/S-5 will enter access into JPAS. The SSA will provide a copy of the approval to HQ AFSOC/SFXI.

3.16. **Processing Request for Access by Retired General Officers or Civilian Equivalent.** Request for access must be submitted to SSA prior to the access requirement, using AF Form 2583. Host organization security manager is responsible for submitting request and maintaining a file until access is no longer needed.

3.22. **Access to North Atlantic Treaty Organization (NATO) Classified Information.** Coordinate temporary NATO access with the SSA. Prior to temporary NATO access, ensure NATO briefings are conducted and documented using AF Form 2583 in accordance with AFI 31-406, Paragraph 4.9. and AFSOCI 33-302.

3.27.1. Investigations are submitted based on the requirements established in AFI 33-119, Paragraph 9.2.5. DOD 5200.2-R and AFI 31-501. Commanders designate information technology (IT) access levels as IT1, IT 2, or IT 3 and code the UMD accordingly using criteria as follows:

3.27.1.1. (Added) IT-I positions. Those positions in which the incumbent is responsible for the planning, direction and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

3.27.1.2. (Added) IT-II positions. Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the IT-I category to ensure the integrity of the system.

3.27.1.3. (Added) IT-III positions. All other positions involved in computer activities. In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system.

3.27.2. Unit security managers provide the results of investigations or changes in eligibility status and identifies those individuals who meet the investigative criteria in accordance with AFI 33-119, Paragraph 9.2.5. 1 SFS/S-5 does not grant or deny access to IT systems. Access to IT systems is granted by 1 CS.

3.27.3. 1 SFS/S-5 conducts security police records checks through Security Forces Management Information System (SFMIS) as part of the interim AIS process. Security managers (SM) will provide investigation status and sign all LAN applications. Security managers verify existing clearances through JPAS or initiate interim clearance requests and forward results back to the unit work-group manager.

3.28.1. (Added) See Paragraph **5.6.1.1. (Added)**

5.1.1.1.1. (Added) Completed PSI paperwork is submitted to an authorized requester (SSA) within 14 days of date on AF Form 2583. The authorized requester will not accept PSI paperwork when dates on AF Form 2583, SF Form 86 or as applicable, are older than 30 calendar days.

5.1.1.1.2. (Added) Initial civilian PSI completed paperwork is submitted to the CPF. CPF will not accept PSI paperwork when dates on the AF Form 2583, SF Form 85, SF Form 85P, SF Form 86, or FD 258, as applicable, are older than 30 calendar days.

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 unit security operating instructions. Refer to the ISPM for minimal requirements.

5.1.1.2.3. (Added) Advise commanders or staff agency chiefs 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 PSIs for their respective units through JPAS. Track exact status of each submitted investigation or suspense for submission and report to the Information Security Program Manager (ISPM) upon request. In-process, check status of non-disclosure agreement NDA (SF 312) and indoctrinate all unit personnel. Post JPAS personnel rosters in their security manager's handbook every 30 days.

5.1.1.2.7. (Added) Review all PSI for errors, before they are submitted to 1 SFS/S-5 representatives. SMs are responsible for ensuring unit personnel submit their PSIs accurately and on-time.

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

5.1.1.2.9. (Added) Check investigation status of all projected inbound personnel prior to arrival on station. SMs also check investigation status of newly assigned personnel during unit in-processing, and request interim clearances for all eligible personnel.

5.2.1. Authorized requestors at Hurlburt Field are 1 SFS/S-5, 1 SVS/SVA and 1 MSS/DPC. 1 SFS/S-5 process initial and periodic reinvestigations (PRs) for military and National Agency Checks for uncleared contractors and periodic reinvestigations for civilian personnel. 1 SVS/SVA processes NACs for employees with child care responsibilities and 1 MSS/DPC will process all initial civilian investigations. Requesters must have a level 5 JPAS account to perform base level account maintenance. e-QIP will be used to submit personnel security investigations PSIs for access to classified information to OPM.

5.2.3. Authorized Callers. The installation security program manager (ISPM) identifies personnel authorized to call the Air Force Central adjudication Facility AFCAF. Before calling the AFCAF, the authorized requester must have the subject's full name, social security number, dates and breaks of service, and any current clearance information from the clearance access verification system CAVS. After receiving information from the AFCAF, the authorized requester will record the data in the remarks section of CAVS.

5.4. **Request Procedures.** Manual fingerprints are no longer authorized for official government investigations. All applicants for investigation will be fingerprinted by authorized requestors using the digital fingerprint equipment at 1 SFS/S-5. Fingerprints must be transmitted electronically to OPM.

5.6.1.1. (Added) Procedures for PSIs and PRs are as follows:

5.6.1.1.1. (Added) Unit security managers are responsible for notifying individuals who are due an initial or PRs.

5.6.1.1.2. (Added) Individuals have 45 days from the date notified to submit PSIs to the SSA, no extensions will be granted unless the member is deployed. Deployed individuals have 45 days from date of return to submit PSIs.

5.6.1.1.3. (Added) Commanders will suspend access to classified information on any individual who fails to submit a PSI within 45 days of notification. Access will be suspended in writing and the individual debriefed using Air Force Form 2587, Security Termination Statement. Provide 1 SFS/S-5 a copy of the suspension letter and AF Form 2587. Access may be reinstated upon submission of an accurate PSI application.

5.6.2. SMs will review all PSI packages to ensure they are error free. SMs must not rely on the e-QIP program to validate packages.

7.1.2.1. Route unit manning document UMD change/requests through the servicing security activity (SSA) to servicing manpower office. Include name and grade of person occupying position number. Special security office (SSO) approves all requests for sensitive compartmented information (SCI) coded personnel security investigation request (PSIR) changes. PSIR codes not authorized by AFSC or listed on the UMD requires AFSOC/CV written approval.

7.1.2.2. Each organization must conduct an annual review to determine the accuracy of position coding. The last AF-wide directed review was conducted in May 04. Reviews will be conducted each May. Post review results in the SM's handbook.

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 or an interim clearance has been approved and entered into JPAS.

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) Commanders grant access to classified information and SMs record access in JPAS. Granting access to classified is based on mission needs, security clearance eligibility, signed SF 312 and need to know.

7.1.2.6. (Added) Commanders grant access to classified information by the SM "Indoctrinating" the member through JPAS. Initial and refresher training documentation must be on file to support access authorization.

7.3.1. The use of TDY orders for verification of clearance data is discouraged due to the frequency and possibility of errors.

7.4. Investigative Requirements for Sensitive Programs. JPAS replaced Sentinel Key on 20 June 2003. Non-SCI, JPAS account manager at Hurlburt Field is 1 SFS/S-5. JPAS account manager for SCI is AFSOC/SSO. Use of JPAS is mandatory for all SMs and requesters at Hurlburt Field.

7.4.2.5. Before access to JPAS is granted, the following must be accomplished:

7.4.2.5.1. (Added) SMs will complete a system access request (SAR) form and joint integrated training application (JITA on-line training) with printed certificate for level 6 access. The base personnel security office will provide localized training in lieu of JITA on-line training if the web site is unavailable. Copies of SAR and certificate will be forwarded to 1 SFS/S-5 prior to security managers being granted JPAS access. The servicing security activity (SSA) will verify the member meets the requirements for JPAS access.

7.4.2.5.2. (Added) Account managers (Level 5) and SMs (Level 6) must at a minimum possess a NACLC for active duty military and reserves or ANACI investigation for civilians

7.4.2.5.3. (Added) Completion and passing the SM and/or JITA computerized training course provided on JPAS web page. Additional training will also be provided by the ISPM during initial SM training. 1 SFS/S-5 will provide localized training in lieu of JITA on-line training if the web site is unavailable.

7.4.2.5.4. (Added) Level 5 access will only be given to military/civilian personnel working in the information, personnel, and/or industrial security programs.

7.4.2.5.5. (Added) Level 6 access will only be given to personnel performing duties as SM. All other positions must be approved by the ISPM.

7.4.2.5.6. (Added) Access will not be given to contractors. Facility security officers control JPAS access for all contractor personnel.

7.4.2.6. Requesting JPAS access:

7.4.2.6.1. SMs 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.

7.4.2.8. JPAS Management:

7.4.2.8.1. (Added) The base 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. All account holders not listed on a current SM's appointment memo will have their accounts deleted from the JPAS system.

7.4.2.8.3. (Added) Personnel found abusing their JPAS access will 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 1 SFS/S-5 and/or designated representatives. If the issue cannot be resolved locally, 1 SFS/S-5 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 personnel data errors through JPAS will not correct the database.

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

7.4.2.8.8. (Added) 1 SFS/S-5 or SSO determines the number of users and the access level for each user.

7.4.6. (Added) SMs maintain current monthly JPAS security clearance listings and share listing with applicable security focal points. Unit SMs should access JPAS periodically for updates and take appropriate action when necessary. SMs will notify the SSA for assistance, when efforts to correct JPAS deficiencies fail.

8.2.1.3. SSA or SSO will notify unit commanders upon receipt of derogatory information and request security information file (SIF) consideration. Commanders have 20 days to make a decision and respond in writing. If 1 SFS/S-5 and unit commander or staff agency chief disagree on whether a SIF should be established the 1 SOW/CC will make the final determination.

8.2.1.4. Commanders must suspend an individual's access to classified information, LAN and unescorted entry to restricted or controlled areas when a SIF is established or suitability determination is made as a result of an on-going investigation. Member must be placed on the control roster or have an unfavorable information file (UIF) established.

8.2.1.5. When establishing a SIF or suitability determination on civilian personnel, unit commanders must also inform the labor and employee management relations section of the civilian personnel flight or element.

8.2.1.10. (Added) The subject's commander notifies the SIF OPR 30 days prior to any PCS, PCA, or TDY. The commander provides written updates as required about the status of the SIF. These updates will contain the status of the commander's reviews and recommendations, along with the estimated time of SIF completion. The goal is to forward all SIF information and recommendation for closure action to AFCAF within 45 days of SIF establishment. Except for brief periods of review, commanders are not authorized to maintain SIF correspondence or files within their unit. The SIF OPR at Hurlburt Field maintains SIF files.

8.2.2.3. OPR for secret and top secret SIFs is the SSA (1 SFS/S-5, 884-619). OPR for SCI access SIFs is AFSOC/SSO, 884-6583.

8.2.2.4. Establishing agency (SSA or SSO) notifies 1 SOW/CC when a SIF is established using memorandum in AFI 31-501, Attachment 18 or electronic equivalent (email).

8.7. Security Clearance Reinstatement. Submit reinstatement requests through SIF OPR (SSA or SSO). Request should be submitted with commander's explanation on how the individual's behavior has improved and the appropriate documentation corresponding to the reason(s) for the denial or revocation.

8.9.1. Unit commanders contemplating disciplinary or administrative action against military members or civilian employees that could lead to discharge or removal with secret or top secret access, must notify the SSA for SIF consideration and/or action. Provide information identified in AFI 31-501, Paragraph 8.9.1.1. through 8.9.1.7. This section applies to all Hurlburt assigned personnel.

9.1.1.2. Commanders, first sergeants, supervisors and SMs should work together as a team to review the standards of DoD 5200.2-R, Chapter 2, any time an individual is involved in an offense meeting this criteria. When in doubt, consult the personnel security office for assistance.

9.3. **Initial Briefings and Refresher Briefings.** Initial and refresher security briefing on the Hurlburt information security web page <https://intranet.hurlburt.af.mil/sow/1msg/1sec/index> html will be used for this purpose.

9.5. **Termination Briefings.** AF Form 2587, Security Termination Statement, will be maintained for 2 years from date of separation by the unit executing the debrief.

Attachment 27 (Added)**SAMPLE REQUEST TO ESTABLISH A SECURITY INFORMATION FILE (SIF)**

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR 1 SFS/S-5

FROM: Commander's Full Address

SUBJECT: Request Establishment of Security Information File (SIF), re: (Last Name, First, Middle, Rank, SSAN).

A27.1. (Added) Request a SIF be established on (Individual).

A27.2. (Added) I have become aware of the subject's involvement in _____ (be specific). After review of DoD 5200.2-R, paragraph 2-200, Appendix I, and AFI 31-501, Chapter 8, it is determined that further evaluation is needed to determine the subject's eligibility to retain access to classified information/ unescorted entry to restricted areas and Local Area Network (LAN).

A27.3. (Added) (SUBJECT) has been placed in a nonsensitive position and all access to the LAN, classified information and or unescorted entry to restricted areas has been withdrawn (suspended) in accordance with AFI 31-501. (If applicable). The special access program manager (DOS/NATO/CNWDI) has been notified that a SIF has been established on the subject. (any of the following as pertinent).

A27.4. (Added) There is a report of investigation ROI. Name of agency conducting the investigation _____. Date of ROI _____.

A27.5. (Added) Subject has been referred to military equal opportunity (MEO). Date of referral is _____.

A27.6. (Added) Mental health will be conducting an evaluation of the subject. Date of referral is _____.

A27.7. (Added) Subject was given disciplinary action for this incident. Type of disciplinary action _____ (e.g., Article 15).

A27.8. (Added) A courts-martial is projected for this individual: (Date).

A27.9. (Added) Subject was placed in appellate leave status: (Date).

A27.10. (Added) The subject's present date eligible retirement or separation (DEROS) date is _____.

A27.11. (Added) We (do/do not) intend to discharge the subject in accordance with AFI 36-3206, Administrative Discharge Procedures for Commissioned Officers, or AFI 36-3208, Administrative Separation of Airmen.

A27.12. (Added) I will provide your office with status updates. Our POC is (name and phone number).

Commander's Signature Block

Attachments:

1. Adverse Security Determination.
2. AF Form 2583 (Only if special access is being withdrawn).
3. AF Form 2586.
4. AF Form 2587.

NORMAN J. BROZENICK, JR., Colonel, USAF
Commander