

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



**AIR FORCE INSTRUCTION 31-501
AIR FORCE MATERIEL COMMAND
Supplement 1
26 FEBRUARY 2004**

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: HQ AFMC/MS (SFXP) (Ms. Sherri Dolan)

Certified by: HQ AFMC/MS
(SFX) (Mr. Francis L. Cooper)

Supersedes AFI 31-501/AFMCSup1, 1 June 1995

Pages: 4
Distribution: F

AFI 31-501, 1 Aug 00, is supplemented as follows:

This supplement is applicable to US Air Force Reserve units and personnel tenant on AFMC installations.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

It aligns its guidance with the revised Air Force Instruction 31-501, 1 August 2000, *Personnel Security Program Management*. Revision includes updating of office symbols; Joint Personnel Adjudication System (JPAS) as the replacement for SENTINEL KEY (SK); Adjudication Management System (AMS) is now the Joint Adjudication Management System (JAMS); Clearance and Access Verification System (CAVS) is currently the Joint Clearance and Access Verification System (JCAVS); and Personnel Security Investigation coding to replace Security Access Requirement (SAR) code.

1.1.2. Submit requests for waivers, inquiries, and recommendations for changes through the servicing ISPM to HQ AFMC/MS(SF), 4225 Logistics Avenue, Bldg 266, Rm N208, Wright-Patterson AFB OH 45433-5760.

2.5. **Authorized Personnel Security Investigative Agencies.** Effective 1 Oct 03, OPM will conduct all DoD military and civilian Personnel Security Investigations (PSIs).

3.12.1. Servicing ISPM submits Limited Access Authorization (LAA) requests for a personnel security investigation to HQ AFMC/MS(SFXP) for approval.

3.24.10.1. (Added) The security manager must ensure a contractor employee has the proper personnel security investigation (PSI) before signing AF Form 2586, Unescorted Entry Authorization Certificate. If there is no record in JPAS, contact the ISPM for assistance in checking Defense Industrial Security Clear-

ance Office (DISCO) records. Submit PSI to the appropriate investigative agency if there is no record of investigation.

3.27.3.7.3. (Added) Unit commanders are responsible for favorable suitability determinations. The commander will use the adjudication guidelines in DoD 5200.2-R, Section 2-200.

3.28. **Periodic Reinvestigations.** Personnel in positions requiring personnel security investigations will submit the appropriate update before the expiration date of the investigation. Top Secret positions must be current within 5 years and Secret positions must be current within 10 years. Failure to complete the appropriate reinvestigation shall result in termination of the individual's security clearance or assignment to sensitive duties.

4.1. **Prior Federal Civilian Investigations.** Investigations conducted on a current or former military member or DoD contractor with the appropriate investigation are also acceptable for granting immediate access to classified information, entry to restricted areas, access to an unclassified LAN system, or for the NAC portion of background checks for individuals in child care service positions.

4.1.1.5. (Added) If the information is not in JPAS, contact the employee's former supervisor and/or security manager (or similar official) to determine if the individual had a security clearance and the level of access held. If possible, obtain written data relating to the security clearance/access such as the date and type of investigation and how long the employee worked at the activity. Ensure individual has no adverse information in their employment records or former unit's security records.

5.1.1.2. (Added) Unit security manager will monitor all personnel security investigations through JPAS. The ISPM will review the Periodic Reinvestigations (PRs) report during program reviews to ensure PRs are being monitored and submitted accordingly.

5.2.2. Servicing ISPM submit requests for designation as authorized requesters to HQ AFMC/MS(SFXP). Provide justification for the need to be an authorized requester, complete organizational title, symbol, organizational PASCODE, mailing address, point of contact, and commercial and DSN telephone numbers.

7.1.2.1. IAW SAF/AA Memo, 11 Oct 02, Personnel Security Investigations Requirements, position coding will be assigned by the type of investigation required for mission purposes vs security clearance requirements. The term security access requirement (SAR) has been replaced with position coding. Upgrade of a position from Secret to Top Secret or identification of a new Top Secret requirement, requires 3-Star/civilian equivalent approval.

7.1.2.1.1. (Added) AFMC/CV may delegate authority to center commanders to approve new Single Scope Background Investigation (SSBI) requirements. This will be determined on a case-by-case basis. The center commander may submit their request to AFMC/CV and a courtesy copy to HQ AFMC/MS(SF).

7.1.2.1.2. (Added) Submit a courtesy copy for any new/upgrade Single Scope Background Investigation (SSBI) requirement to HQ AFMC/MS(SFXP).

7.2.3. (Added) A select group of Air Force Specialty Codes (AFSCs) for officers and enlisted personnel have a mandatory SSBI requirement. The AFSC list is also applicable to DoD civilian positions. The list is updated periodically and the ISPM is responsible for maintaining the most current listing.

7.4. **SENTINEL KEY.** Joint Personnel Adjudication System (JPAS) is the sole repository for security clearance/investigation data. The Joint Adjudication Management System (JAMS) and the Joint Clear-

ance and Access Verification System (JCAVS) are the two sub-systems in JPAS. JAMS provides the Central Adjudication Facility (CAF) a single, integrated Information System to assist the adjudication process. As the adjudicators input investigative information into JAMS it becomes "real time." JCAVS provides DoD security personnel the ability to instantaneously update other JCAVS users with pertinent personnel security clearance and access information in order to ensure the reciprocal acceptance of clearances throughout DoD. This system is designed for security managers. HQ AFMC/MS(SF) is the JPAS account manager for the MAJCOM.

7.4.2.5. Contractors that perform security functions have limited access to and limited use of JPAS. The servicing ISPM must ensure the contractor has a favorable investigation before accessing JPAS. ISPM maintains a list of contractors that have access to JPAS. Include the contractor's name, company, SSN, and phone number. The access level may be the same as a security manager (level 6) or lower.

7.4.2.5.1. (Added) An individual must have a National Agency Check, Local Agency Checks and Credit (NACLC) or Access National Agency Check and Inquiries (ANACI) investigation completed before a JPAS account is established.

7.4.2.5.2. (Added) Servicing ISPM submit access request forms for base level 5 access to HQ AFMC/MS(SFXP) for approval.

7.4.2.6. There are 8 User Levels in Joint Clearance Access Verification System (JCAVS). These levels are defined as follows:

7.4.2.6.2. LEVEL 2 - SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters. Personnel Security Management Net (PSM Net) is determined by the responsible SOIC or designee. (Read and Write Access - SSBI) **M-1 Criteria.

7.4.2.6.3. LEVEL 3 - SCI security personnel at echelons subordinate to Level 2 at a particular geographic location (installation, base, post, naval vessel). PSM Net is determined by the responsible SOIC or designee. (Read and Write Access-SSBI) **M-1 Criteria.

7.4.2.6.4. LEVEL 4 - Non-SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters. PSM Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLC/ANACI).

7.4.2.6.5. LEVEL 5 - Non-SCI security personnel at echelons subordinate to Level 4 at a particular geographic location (installation, base, post, naval vessel). PSM Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLC/ANACI).

7.4.2.6.6. LEVEL 6 - Unit security manager (additional duty) responsible for security functions as determined by responsible senior security official. (Read and Write Access - NACLC/ANACI).

7.4.2.6.7. LEVEL 7 - Entry control personnel. Individuals who grant access to installations, buildings, etc. Varies according to organizations. (Read Access - NACLC/ ANACI).

7.4.2.6.8. (Added) LEVEL 8 - SCI Entry control personnel. Individuals who grant access to SCIF installations, buildings, etc. Varies according to organizations. (Read Access - SSBI).

7.4.2.6.9. (Added) LEVEL 10 - Visitor Management. Level 10 users will have the same view of the JCAVS person summary as a JCAVS Level 7 user. They will receive visit notifications when their SMO is being notified of a visit. A Level 10 user may not be an account manager, create or delete an account at any level.

- 7.4.2.8.1. (Added) Servicing ISPM will manage their local JPAS account (Level 5, 6, and 7).
- 7.4.2.8.2. (Added) Servicing ISPM will review JPAS accounts quarterly for accuracy.
- 7.4.2.8.3. (Added) Personnel found abusing their JPAS access will have their access removed (e.g. open a JPAS account for an individual that is not authorized). The center commander must approve request for reinstatement.
- 7.5.1. (Added) IAW HQ USAF/XOF memo, 25 Nov 02, positions identified for deployment will be assigned a NACLIC, requiring access to Secret information for the in-country threat briefing. SSIBs will not be authorized for purposes of Top Secret “just in case of” deployment.
- 7.6.1. Authorized requesters send changes, deletions, or additions to their list of authorized callers to HQ AFMC/MS(SFXP). Limit telephone calls to emergency situations. Use JPAS for tracer transactions in routine situations.
- 8.2.1.4.1. (Added) Commanders/staff agency chiefs record suspension of an individual’s access or unescorted entry to restricted areas on an AF Form 2587 and send to the servicing ISPM for inclusion in the Security Information File (SIF) file.
- 8.2.2.5.1. Employment suitability determinations are required as part of SIFs for civilian employees. Commanders or staff agency chiefs are responsible for these determinations with the assistance of the Civilian Personnel Flight (CPF).
- 8.6.2. Submit appeals through the servicing ISPM.
- 8.6.4. Submit rebuttals through the servicing ISPM.
- 8.7. **Security Clearance Reinstatement.** Submit all requests for reinstatements through the servicing ISPM.
- 9.1.1.1.1. (Added) Include during recurring security training each individual’s responsibility for identifying and reporting derogatory information IAW DoD 5200.2-R, Section 9-104.
- 11.1.4.1. (Added) Identify servicing ISPM oversight procedures in local supplement.

CHERYL L. DOZIER, Colonel, USAF
Chief, Security Forces
Directorate of Mission Support