

**BY ORDER OF THE INSTALLATION COMMANDER
HEADQUARTERS 377TH AIR BASE WING (AFMC)
KIRTLAND AIR FORCE BASE, NEW MEXICO 87117-5000**

**KAFBI SUPPLEMENT 1
AFI 31-601
15 May 2006**

Operations

INDUSTRIAL SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: 377 SFS/SFAID (Mr. Manuel D. Camarena)

Certified by: 377 SFS/CC
(Maj Martin L. Rothrock)

Pages: 5

Distribution: X

This supplement applies to all personnel assigned to Kirtland Air Force Base (KAFB) including associate units, contractors, and transiting units to the installation.

Summary of Revisions: This document has significant changes and must be completely reviewed. It updates procedures and aligns guidance with AFI 31-601, 22 Nov 00, and Air Force Materiel Command (AFMC) Supplement 1, 28 Jun 01.

1.4. Send requests for interpretation, clarification, or waiver through 377th Security Forces Squadron, Administration (377 SFS/SFA) to the Information Security Program Manager (ISPM), 377th Security Forces Squadron Commander (377 SFS/CC). 377 SFS/CC will respond or forward to Headquarters Air Force Materiel Command Security Forces (HQ AFMC/MSF).

1.5.3.1. (Added) 377 SFS/CC is responsible for the KAFB Industrial Security Program.

1.5.5.1. The Senior Intelligence Office (AFRL/DETI) and Special Security Office (SSO) handle intelligence requirements for all AFMC units and associated units requiring support.

1.5.6. The 377th Communications Division (377 MSG/SC) is responsible for Automated Information Systems (AIS), Communications Security (COMSEC), Emissions Security (EMSEC), and For Official Use Only (FOUO) information controlled and managed in accordance with the Freedom of Information Act Program at KAFB.

1.5.7. DELETED.

1.5.9. The Installation Commander (IC) has designated the ISPM, 377 SFS/CC, as the authority for authorizing and/or granting Department of Defense (DoD) contractors access to the installation and for providing appropriate security supervision over the on-base contractor operation and its personnel.

1.6.1.2. The 377th Security Forces Squadron, Industrial Security Office (377 SFS/SFAID) will initiate the Visitor Group Security Agreement (VGSA) and track completion for all Integrated and DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)* visitor groups on KAFB.

1.6.1.2.1. Primary Security Managers will notify 377 SFS/SFAID when contractors performing on unclassified efforts are on site with their organization for periods of 30 days or more continuously. The notification should include the name of the company, contract number, number of employees, and duration of performance and will be submitted to 377 SFS/SFAID no later than 10 days prior to performance beginning. A consolidated list of contractors performing on unclassified efforts will be submitted to 377 SFS/SFA by 01 September of each year.

1.6.1.4. The IC has designated the ISPM, 377 SFS/CC, as the authority to perform Industrial Security Program oversight for on-base contractor operations and personnel. The 377 SFS/SFAID manages this function for the ISPM.

1.6.2.2. 377 SFS/SFAID must review all contracting issued DD Form 254, **Department of Defense Contract Security Classification Specification**, for compliance.

1.6.2.3. 377 SFS/SFAID reviews all DD Form 254s to ensure security is adequate to protect classified information.

1.6.2.4. 377 SFS/SFAID monitors and tracks the completion of DD Form 254s. The Primary Security Manager will be tasked collectively with the Contracting Officer (CO) to ensure the appropriate program/project manager completes the review and notifies 377 SFS/SFAID of action taken. As a minimum, review and revise the classification/declassification security guidance every five years or as circumstances require.

1.6.2.5. 377 SFS/SFAID will initiate or prepare all VGSA and track completion for all integrated and NISPOM visitor groups on KAFB.

1.6.5.1. 377 SFS/CC is the ISPM responsible for the oversight and administration of the Industrial Security Program for KAFB. 377 SFS/SFAID manages the program for the ISPM.

1.8.2.2. Guidance for reporting security violations is contained in the VGSA.

2.1.3.4. The CO and 377 SFS/SFAID verify facility security clearances (FCLs) and level of safeguarding through the Defense Security Service (DSS) Secure Web Site or DSS Central Verification Activity for all DD Form 254s. CO may contact 377 SFS/SFAID for assistance in verification of the FCL.

3.1. Security training requirements are contained in the VGSA.

3.1.4. Air Force unit security managers or security officers will provide information security program training (initial, refresher, and annual) and other security awareness support to integrated visitor groups. The AF activity, working in concert with the ISPM, will incorporate language into the VGSA, which requires visitor group personnel to attend and/or receive

information security training per DoD 5200.1-R and AFI 31-401. Unit security managers will ensure integrated visitor group personnel are included in their security education program. In addition, unit security managers will ensure initial, refresher, and annual training for integrated visitor groups is completed and documented.

4.1.2. AF program, project officers, or activity point of contacts must involve 377 SFS/SFAID early in the acquisition process when contracts require contractor access to classified or unclassified sensitive information or enhanced physical security for products under the contractor's control.

4.2.4. 377 SFS/SFAID will review and coordinate on all DD Form 254s for Contractor Engineering and Technical Services contracts awarded by KAFB activities.

4.3.1. 377 SFS/SFAID reviews the initial draft and final DD Form 254 for the ISPM.

4.5.5. The VGSA is signed by the organization ISPM/377 SFS/CC, security manager, program manager, and the company representative (typically facility security officer (FSO)). A copy of the completely signed document is forwarded to all parties.

5.1. The ISPM designates on-base visitor groups as cleared facilities, integrated visitor groups, NISPOM visitor group, or intermittent visitors on a case-by-case basis, dependent upon the type of support provided and the performance locations.

5.5. The government program manager, project manager or AF activity will notify 377 SFS/SFAID and the applicable CO in writing within 10 calendar days of termination and/or when the VG's contractual services has been completed.

5.6. The government program manager, project manager or AF activity will notify the CO and 377 SFS/SFAID 30 days prior to contract completion or shutdown on KAFB in order to review contractor's operations ensuring proper disposition of classified materials per DoD 5200.1-R, AFI 31-401, and the applicable VGSA.

6.1.2. 377 SFS/SFAID will conduct industrial security reviews of on-base integrated visitor groups annually.

6.2.1. 377 SFS/SFAI and 377 SFS/SFAID will conduct security reviews of on-base integrated visitor groups collectively with the AF activity. AF activity will include all sponsored on-base integrated visitors groups in their self-inspection.

6.2.4. 377 SFS/SFAID will maintain files, for the ISPM, with required documentation on all on-base visitor groups. The organization security manager will maintain six-part folders for each individual contractor. At a minimum, the six part folder will contain:

6.2.4.1. *Tab 1:* Signed copy of the DD Form 254 and any revisions.

6.2.4.2. *Tab 2:* Signed copy of the VGSA. 377 SFS/SFAID will maintain a signed copy of the VGSA for all on-base visitor groups.

6.2.4.3. *Tab 3:* Current listing of the key on-base management officials or representatives. At a minimum, the list should include the name, phone number, and address of the contract security focal point, government project manager and FSO.

6.2.4.4. *Tab 4:* Copy of last annual ISPM program review.

6.2.4.5. *Tab 5:* Copies of last two self-inspection reports. The annual program review can be used to substitute for one of the self-inspections. **NOTE:** SFS/SFAID will not maintain a copy of the self-inspection report for integrated visitor groups.

6.2.4.6. *Tab 6:* Current JPAS Visit Request or Visit Authorization Letter (VAL) IAW DoD 5220.22-M, Chapter 6, Section 1, 6-103 (No JPAS Access) and DoD 5200.1-R, C6.2.3.

6.2.6.1. 377 SFS/SFAID will maintain a copy of the required files/records for NISPOM visitor groups, with the exception of the self-inspection. However, the self-inspection report will be reviewed during program reviews and documented in the program review report.

6.2.7. 377 SFS/SFAID will conduct the industrial security review of all on-base visitor groups except visitor groups with oversight from other agencies.

7.3.2. Access by Visitors. JPAS is the primary source for confirming access eligibility for DoD and DoD contractor personnel. Visit authorization letters will not be used to pass security clearance information unless JPAS is not available. [Reference DoD 5200.1-R, C6.2.3.] The contractor Home Office Facility will submit a visit request to the AF activity and CO or designated representative requesting the visit.

7.3.2.1. Incoming Visit Requests. AF activity visit hosts serve as the approval authority for visits to their activities. AF activity visit hosts use JPAS to confirm security clearances of DoD personnel, including DoD contractors. AF activity visit hosts will in-process/out-process DoD contracted personnel via JPAS for continued verification of contracted personnel security clearances.

7.3.2.2. DELETED

7.3.2.3. DELETED

7.3.2.4. DELETED

7.3.2.5. DELETED

7.3.2.6. DELETED

7.3.3. DELETED

9.1.3. Personnel security investigations for uncleared contractor employees who require access to unclassified government information systems are processed through 377 SFS/SFAIP as necessary.

TERRENCE A. FEEHAN, Colonel, USAF
Commander