

AFI31-401/439SUP1

BY ORDER OF THE COMMANDER 439<sup>TH</sup> WING

AIR FORCE INSTRUCTION 31-401

1

21 March 2001

Security

MANAGING THE INFORMATION SECURITY PROGRAM

OPR: 439 SFS/SFA (Capt Rodney Walker)

Certified by: 439 SPTG/CC (Lt Col James P. Joyce)

Supersedes AFI 31-401, 22 July 1994 and AFI 31-401/439 WG Sup, 8 June 1999

Pages: 4/Distribution: F

---

The OPR for this supplement is 439 SFS/SFA (Capt Rodney Walker). This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-401, 1 January 1999. The AFI is published word-for-word without editorial review. 439 Airlift Wing (AW) supplementary material is indicated by "439 AW" in boldface type. This supplement describes 439 AW procedures to be used in conjunction with the basic instruction. Upon receipt of this integrated supplement, discard the standalone Air Force basic. This supplement applies to all organizations and cleared contractors assigned or attached to Westover Air Reserve Base.

### ***SUMMARY OF REVISIONS***

This revision identifies responsibilities and procedures to be followed by cleared contractors throughout; includes industrial security inspections (paragraph 5.5.1.6); and establishes procedures for personal electronic devices (paragraph 5.11.4). A (I) indicates revisions from the previous edition.

1.3.4. The 439 Security Forces Squadron commander (439 SFS/CC) is the Westover ARB information security program manager (ISPM) and Industrial Security, Servicing Security Activity (SSA). The focal point for the base ISPM is the Information, Personnel and Industrial Security Section (SFA).

1.3.5.1. Unit commanders appoint a primary and alternate security manager and forward appointment letters to SFA for inclusion in the unit's file. The primary security manager should be an Air Reserve Technician or full time civilian employee. A company security manager will be appointed by cleared contractors and identified to SFA.

1.3.6.6. Semiannual security inspections will be conducted by all units and cleared contractors in May and September of each year. Self inspection reports will be forwarded to SFA not later than 30 days after the inspection for review and inclusion in the unit's file maintained by the ISPM. The unit commander will appoint an E-7 or GS-6 or above to conduct this review. Cleared contractors will

complete the inspection in accordance with National Industrial Security Program Operating Manual (NISPOM) requirements. All results and suggested corrective measures must be approved and signed by the unit commander/company security officer prior to forwarding the report. Units and cleared contractors not maintaining classified information will conduct self inspections annually in September and forward the reports to SFA. The unit commander will make the determination for the unit and coordinate with the ISPM on the frequency of the self inspections.

2.3. Send challenges to classification of AF information through SFA to the originator.

2.3.3. Send requests for reclassifying information through SFA.

5.5. The unit security manager or cleared contractor security officer will ensure each SF 312, **Classified Information Nondisclosure Agreement (NDA)**, is properly prepared and executed. In addition, the top of each SF 312 will be annotated by all military members with the signatory's military rank and functional address symbol.

\*5.5.1.6. Each completed SF 312 will be staged by the respective activity's unit security managers/cleared contractor security officer and disposed of as indicated below. Unit, staff agencies and cleared contractor compliance with the NDA policy will be addressed during the unit semiannual inspection, annual program reviews, and industrial security inspections

5.5.1.7. For military personnel, the original SF 312 must be forwarded to SFA. Maintain a copy of the signed SF 312 until the Automated Security Clearance Approval System roster has been updated.

5.5.1.8. For civilian employees, the original must be forwarded to AFRC, Randolph AFB TX, to be updated in the personnel data system and filed in the employee's Official Personnel File. For cleared contractor employees the original will be filed with the Facility Security Officer.

5.5.1.9. When a person refuses to sign an NDA, send an information copy to SFA.

5.10.1.1. Establishment of top secret control (TSC) accounts will be reported to SFA. This notification will include the name, office symbol, and telephone number of both the primary and alternate TSC officers.

5.10.1.3.1. 439AW/CC is responsible for designating officials to conduct inventories as required.

\*5.11.4. (Added) Classified custodians, or those in charge of classified briefings, should initiate procedures to preclude the introduction of Personal Electronic Devices (PEDS) into a classified storage/discussion/processing area. PEDS are described as Personal Digital Assistants (PDAS), palm tops, hand-held computers and workstations, web based enhanced cell phones, two-way pagers, and

wireless e-mail devices. Classified custodians will, at a minimum, ensure that all PEDS are turned off prior to granting entry to any secure area where classified information may be stored, processed, or discussed.

5.14.1. The Westover Command Post (CP), located in building 7091, is the designated overnight storage facility for in-transit classified information. Precoordinate when possible.

5.14.2. Classified equipment (when removed from the aircraft) can be stored at the CP. If the equipment is too large for storage at the CP, coordinate with SFS for temporary storage.

5.15.1. Send requests for approval of secure conference facilities through SFA. Contact Detachment 102, AF Office of Special Investigation, Hanscom AFB, MA for a decibel level survey.

5.20.4. (Added) For 439 AW units or cleared contractors, storage of classified information in open or unattended storage areas must be approved by 439 AW/CC. Requests will be coordinated through the base Civil Engineer and SFA. DoD or other service associate units should comply with their parent component directives.

5.24. If locksmith services are not available through Civil Engineering, the unit IMPAC card holder will arrange for the maintenance on a security container or assistance with changing the container combination. The AFTO Form 36, **Maintenance Record for Security Type Equipment**, must be annotated only by a locksmith or certified security personnel. New combination numbers will not be revealed to any contracted locksmiths.

5.24.4. (Added) Coordinate all major construction of facilities having vaults and secure storage areas with your respective staff agency security manager and SFA. Construction criteria is defined in DoDR 5200.1, *DoD Information Security Program Regulation, Appendix F*. All work requests for modification of containers, vaults and secure storage rooms must be coordinated with SFA.

5.26.3.2. Run three blank sheets through copiers to clear all latent images.

5.29.2.6. (Added) The central base classified material destruction facility is located in building 7091, Message Center; 439 Communications Squadron is responsible for this facility.

6.8.1. (Added) Coordinate requests for removing classified material from the designated work area during non-duty hours with SFA. Cleared contractors will comply with the requirements outlined in NISPOM, Chapter 5.

6.8.2. (Added) Unit commanders establish procedures for internal controls of secret and confidential information. All personnel assigned to the unit must be familiar with these controls.

6.8.3 (Added) Hand-carrying classified briefing material should be included in the unit's training plan.

8.3.1. The unit supervisors will conduct and document initial and recurring training for each person assigned. Training documentation should be maintained in the security managers handbook. Include dates, topics and names of personnel trained and signatures. Cleared contractors will comply with NISPOM, Chapter 3.

8.7.2.4. (Added) The ISPM will conduct security manager training on general responsibilities within 90 days of receiving an appointment letter of a new security manager. New security managers will be required to attend the Information Security Orientation Course conducted by DSS. Cleared contractor security officers will comply with the training requirements specified in the Visitor Security Agreement. Different topics will be briefed during security managers meetings or via email.

8.9. Recurring training will be conducted at least annually.

9.1.4. (Added) When someone knowingly, willfully or negligently discloses classified information to unauthorized individuals, unit commanders or cleared contractor security officers will forward this information to SFA immediately.

9.2.1. The 439 AW/CC will be notified of units failing to report security violations within the allotted time unless such a delay is unavoidable.

9.3.2.1. The investigative official must be appointed in writing and should be either an officer, a noncommissioned officer E-7 or above, or government service civilian GS-6 or above. The inquiry official must complete their findings within a 30-day period unless a request for extension is granted by the appointing authority. A copy of the appointment letter will be forwarded to the ISPM. Cleared contractors will comply with the requirements contained in NISPOM, Section 1-303.

9.4.1.4. Forward the written investigation with commanders or cleared contractor security official's request for closure to SFA for ISPM approval.

9.6.1.4. (Added) Send requests for waivers of provisions of the security program through SFA.

MARTIN M. MAZICK, Colonel, USAFR

Commander