

**BY ORDER OF THE COMMANDER
AIR EDUCATION AND TRAINING
COMMAND**



**AIR FORCE INSTRUCTION 31-401
AIR EDUCATION AND TRAINING COMMAND
Supplement 1
28 JANUARY 2003**

Security

**INFORMATION 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 AETC/SFI (MSgt R. Newton)
Supersedes AFI 31-401/AETC Sup 1,
14 September 1999

Certified by: HQ AETC/SFI (Mr B. Kilgore)
Pages: 9
Distribution: F

AFI 31-401, 1 November 2001, is supplemented as follows:

In addition to the basic AFI, this supplement will be used in conjunction with DoD 5200.1-R, *Information Security Program*, and DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*. This supplement applies to the Air Force Reserve Command. It applies to the Air National Guard only upon federalization and/or mobilization and when published in the ANGIND 2.

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. Maintain and dispose of records created as a result of processes prescribed in this publication in accordance with AFMAN 37-139, *Records Disposition Schedule*.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

It incorporates training requirements for installation security program managers (paragraphs **1.3.5.2.1. (Added)** and **1.3.5.2.2. (Added)**); prescribes the use of five new AETC visual aids (AETC VAs 31-5 through 31-10) for posting on copiers, fax machines, scanners, and shredders authorized (or not authorized) for reproduction (or destruction) of classified material; and adds guidance for marking special types of materials, to include the permanent marking of each security container (paragraph **5.23.4. (Added)**).

1.3.4.4. (Added) Schedule and conduct security manager meetings semiannually. Meeting minutes will be published and distributed to each unit or staff agency.

1.3.4.5. (Added) Invite (in writing) non-AETC units on AETC installations to participate in the AETC Information Security Program. Ensure oversight requirements are contained in applicable host-tenant support agreements. AETC units located on non-AETC installations will enter into a host-tenant support agreement with the host activity and fully comply with the host-base information security program. In the

absence of a host-tenant agreement, AETC units on non-AETC installations will comply with this supplement.

1.3.5.1. Unit commanders or staff agency chiefs will appoint a primary security manager and as many alternates as necessary and provide a copy of the appointment memorandum to the information security manager (ISPM).

1.3.5.2. In addition to the requirements in Chapter 8 of the basic AFI and this supplement, the following guidance applies to the training of unit and staff agency security managers:

1.3.5.2.1. (Added) Formal enrollment for L6AGU3P071-000, Information Security Distance Learning Course, is limited to ISPMs, the Security Forces Administration—Information Security (SFAI) staff, and civilians in series 080. Requests for the course should be submitted to 342 TRS/DORM, 1001 Gemini Dr, Lackland AFB TX 78236. Enrollment information and criteria is contained in the education and training course announcements (ETCA) at <https://etca.randolph.af.mil/>. ISPMs have 30 calendar days to complete the course.

1.3.5.2.2. (Added) Newly assigned security managers and alternates will notify the ISPM within 15 days of assignment to be scheduled for security manager's training. Prior to attending localized training, security managers must satisfactorily complete the L6AGU3P071-000 (paragraph 1.3.5.2.1. (Added)). Security managers must register through their local ISPM, and they will receive course completion from the base ISPM. Security managers have 60 calendar days to complete the course. Security managers and alternates must complete localized training within 90 days of appointment. ISPMs may make additional copies of the Information Security Distance Learning Course CD-ROM to assist or supplement other localized training efforts.

1.3.6.1. Ensure AETC VA 31-9, *Security Manager Designation*, is posted in conspicuous places within each occupied unit or agency facility. Adding digital photos of the security manager will enhance identification of each security manager.

1.3.6.2. For coordination prior to publication, route draft copies of proposed or revised unit security operating instructions (OI) through the servicing ISPM via AF Form 673, **Request to Issue Publication**, or AF Form 1768, **Staff Summary Sheet**. Provide a final copy of the OI to the ISPM.

1.3.6.10. (Added) Maintain a security manager's book containing the following items, at a minimum:

1.3.6.10.1. (Added) Section 1, the commander's appointment memorandum.

1.3.6.10.2. (Added) Section 2, security manager training certificates.

1.3.6.10.3. (Added) Section 3, the most recent annual program review from the ISPM.

1.3.6.10.4. (Added) Section 4, the last semiannual security self-inspection, with appointment memorandums for the inspecting officials.

1.3.6.10.5. (Added) Section 5, the unit security OI.

1.3.6.10.6. (Added) Section 6, the training section, which contains training materials used for inprocessing and recurring training. This section will also contain validation of training accomplishments.

1.3.6.10.7. (Added) Section 7, sentinel key (SK) security data and rosters.

1.3.6.10.8. (Added) Section 8, information and policy memorandums retained according to the appropriate table and rule in AFMAN 37-139. File the last two semiannual security manager's meeting minutes in this section.

- 1.3.6.10.9. (Added) Section 9, copies of vault or secure room certification, if applicable.
- 1.3.6.10.10. (Added) Section 10, industrial security contracts and related correspondence, if applicable.
- 1.3.6.10.11. (Added) Section 11, miscellaneous items.
- 1.4.1. Unit security management and information security oversight requirements will be incorporated into appropriate HQ AETC/IG inspection checklists and updated on a recurring basis.
- 1.4.2. ISPMs will retain the last two annual program reviews in their management folders.
- 1.4.3. A small volume of classified information is defined as 100 printed pages or less, 3 computer disks or less, 3 CD-ROMs or less, 5 videotapes or less, and 100 sheets of microfiche or less. Exceeding any of these measurements or combining any two of them will constitute a classified account. One hard drive used to store classified material constitutes a classified account.
- 1.4.3.1. In AETC, security managers and alternates will not conduct these inspections.
- 1.4.3.2. (Added) HQ AETC/SFI will prepare and distribute checklists to ISPMs, who are strongly encouraged to localize the checklist. Unit commanders and staff agency chiefs will provide a copy of the semiannual security inspection report to the servicing ISPM. **NOTE:** Program reviews conducted by ISPMs may count as one of the unit's semiannual security self-inspections.
- 1.5.1.1.2. Individuals occupying the following positions are authorized to act for the AETC Commander in certifying requests for access to restricted data via Department of Energy (DoE) Form 5631-20, **Request for Visit or Access Approval**, which includes critical nuclear weapon design information (CNWDI) material in the hands of DoE or federal agencies other than the National Aeronautical and Space Administration: (**NOTE:** This authority will not be further delegated.)
- 1.5.1.1.2.1. (Added) Installation commanders.
- 1.5.1.1.2.2. (Added) Commanders of the following units: 363d and 365th Training Squadrons (TRS), Sheppard AFB; 37th Civil Engineer Squadron (CES), Lackland AFB; 56th CES, Luke AFB; 325th CES, Tyndall AFB; 343d and 342d Technical Training Squadrons, Lackland AFB; Det 3, 366th TRS, Eglin AFB; and 314 CES, Little Rock AFB.
- 1.5.1.1.2.3. (Added) HQ AETC Directorate of Operations, Chief, Technical Training Division (HQ AETC/DOO).
- 1.8.2. Submit the violations and infractions report to HQ AETC/SFI by 10 January and 10 July, each year.
- 2.1.3. In AETC, the following positions are designated as original classification authorities (OCA) up to and including Secret: the AETC Commander (AETC/CC), Director of Logistics (HQ AETC/LG), and Air University Commander (AU/CC).
- 2.3.2. Send an information copy to HQ AETC/SFI.
- 4.9. (Added) **Marking Notebooks, Binders, and Similar Holders.** Notebooks, binders, and similar holders containing classified information will be conspicuously marked with the highest classification of the material contained within. The appropriate classified cover sheet will be affixed to the front and back of the binder, notebook, or holder. Also, the spine on binders, notebooks, or holders will be marked with the overall classification.
- 4.10. (Added) **Marking Envelopes, File Folders, and Dividers in Classified Safes.** Envelopes in classified storage containers containing classified documents will be marked on the front and back with the

highest classification maintained. The tops and bottoms of file folders and dividers will be affixed with the highest level of classification maintained in that record series.

4.11. (Added) **Special Types of Materials.** All electronic media (for example, slides, transparencies, photographs, maps, and charts) will be marked consistent with DoD 5200.1-R, Section 4. All information contained within will be portion marked. If slides are not portion marked, their classifications will be recorded in the "Notes Pages" of the Powerpoint® slide presentation, along with the overall markings present on each briefing slide.

5.5.4. (Added) **Attesting to Security Commitment.** All military and civilian personnel with Top Secret access and/or those with access to special access program material (Top Secret, Secret, Confidential) or sensitive compartmented information must orally attest to their security commitment. (**NOTE:** Contractors are not included at this time.) These personnel will use DoD 5200.1-PH-1 as a guide for conducting verbal attestations and follow the procedures below:

5.5.4.1. (Added) Individuals in Top Secret or special access positions will read paragraph 1 of the SF 312, **Classified Information Nondisclosure Agreement**, and verbally state they understand it and will abide, without equivocation, by its direction.

5.5.4.2. (Added) Two people must witness all attestations. The name of the person making the attestation will be recorded in a memorandum, and he or she will acknowledge receipt by endorsement. Both witnesses will also endorse the memorandum. The unit or staff agency security manager will maintain the documentation, and he or she will provide a copy to the person making the attestation to show as proof for future assignments or accesses.

5.10.1.1. Units will provide a copy of the Top Secret control officer (TSCO) appointment memorandum to the servicing ISPM.

5.10.1.3.1. Units will provide a copy of the annual inventory report to the servicing ISPM.

5.12. **End-of-Day Security Checks.** End-of-day security check procedures will be incorporated into activity OIs. SF 701, **Activity Security Checklist**, is not required in areas that are continuously staffed.

5.15.1. The facility must afford adequate security against unauthorized access, from both physical intruders and sound emissions. Before working with classified components or conducting classified meetings or briefings, wireless products (cell phones, pagers, beepers, hand-held radios, wireless microphones, etc.) must be turned off and placed in a holding area (if available) outside the location where classified components are stored or being briefed. Entry control and perimeter surveillance will be established by posting personnel from the sponsoring activity in and around the room or facility, as necessary. **NOTE:** Security Forces are not responsible for this function, but may assist in the review of unit security plans.

5.17.1. Unit or staff agency certification procedures for classified information processing equipment (for example, copiers, fax machines) will be incorporated into unit security OIs.

5.17.2.1. During annual program reviews, ISPMs will ensure computer systems designated for the processing of classified information are accredited and a current risk analysis is on file. The ISPM will maintain a list of all accredited equipment (to include the serial numbers of each item) in the security manager's handbook, emissions security book, communications security book, or similar record-keeping location.

5.20.2. To reduce or prevent inadvertent access to information, AETC VA 31-10, *Classified Work in Progress*, will be posted in a conspicuous manner when processing such information.

5.20.4. GSA security containers and doors used to store *Top Secret or special access material* must immediately be equipped with locks meeting Federal Specification FF-L-2740, Lock, Combination. By fiscal year 2005, GSA security containers and doors used to store *all other collateral classified material* will be retrofitted with locks meeting Federal Specification FF-L-2740. **NOTE:** The only existing locks that currently meet this specification are X-07, X-08, and X-09 by Mas-Hamilton or Kaba Mas.

5.20.5. (Added) **Storing Classified Material for Other Units or Staff Agencies:**

5.20.5.1. (Added) AETC units or staff agencies may store classified material for other units or staff agencies when the owning unit's volume of classified material or frequency of use does not justify maintaining a security container. The material will be placed in a sealed envelope or container, and the envelope or container will be marked front and back with the highest classification.

5.20.5.2. (Added) The owning agency will provide the storing agency a memorandum with the names, organizational addresses, telephone numbers, and security clearances of personnel authorized access to the envelope or container. The owning agency will review the material quarterly, and the reviewing official will sign and date a review sheet or log attesting that the material is still required.

5.20.5.3. (Added) AF Form 614, **Charge Out Record**, will be used when the material is temporarily removed, and units will establish procedures to ensure all classified material is returned to the storage container before the end-of-day check.

5.20.6. (Added) **Vaults and Secure Rooms.** The structural standards identified in DoD 5200.1-R (Appendix 7) and Military Handbook 1013/1A, *Design Guidelines for Physical Security Facilities*, apply to AETC activities. (Contact HQ AETC/SFI or your local security manager for access to Military Handbook 1013/1A.) Vaults and secure rooms that were certified and approved before January 1997 are still valid and do not require recertification. (**NOTE:** Tenant units on AETC installations that participate in the host base information security program will follow the procedures in this paragraph. Tenant units that do not participate in AETC information security programs will follow their MAJCOM's guidance, and a copy of this guidance will be provided to the host ISPM.) The following guidance applies:

5.20.6.1. (Added) AETC activities should consider building a secure room to store Secret and Confidential materials when necessary. These structures will provide an effective safeguarding capability and eliminate the high costs associated with building vaults.

5.20.6.2. (Added) Compensatory measures are required when vaults or secure rooms do not meet the construction standards in DoD 5200.1-R, (Appendix 7), and Military Handbook 1013/1A, and these measures must be applied before open storage of classified material may be approved. Refer to DoD 5200.1-R, paragraph C6.4.3.1, for supplementary controls involving storage of Top Secret material.

5.20.6.3. (Added) Modifications made to vaults and secure rooms will rescind any previous certification and approval authority for continued open storage of classified materials (per DoD 5200.1-R, Appendix 7). The ISPM and civil engineer must recertify the structural integrity of vaults and secure rooms, even if they were previously built to standards.

5.20.7. (Added) **Certification and Approval.** To openly store classified materials in vaults or secure rooms, the following actions are necessary to obtain certification and approval. The unit or staff agency requiring the secure room or vault will ensure the following actions are accomplished:

5.20.7.1. (Added) The unit or staff agency will submit an OI, outlining procedures for providing protection and positive entry control to the vault or secure room. The ISPM will certify that the plan or OI provides adequate safeguards for the protection of classified material.

5.20.7.2. (Added) Before construction or compensatory measures are included, the ISPM and civil engineer will review new construction or structural modifications to ensure the vault or secure room design meets physical security standards for Secret or Top Secret storage. Once construction or modifications are complete, the ISPM and civil engineer will certify, in writing, whether the facility meets physical security standards.

5.20.7.3. (Added) If the facility meets the standards, no further action is required. If the facility does not meet physical security standards, the unit or staff agency (submitting agency) will send a written plan (via AF Form 1768) for forwarding through the ISPM and civil engineer to the installation commander. The plan package will explain what compensatory measures will be implemented for the level of certification required (Secret or Top Secret) and will address indepth security along with a risk analysis. One copy each of the ISPM and civil engineer physical security reviews will be attached along with floor plans of the facility.

5.20.7.4. (Added) The ISPM and civil engineer will concur or nonconcur with the plan. (If either nonconcur, he or she will provide rationale for the decision and attach it to the package.) In any event, the package will be sent to the installation commander.

5.20.7.5. (Added) The installation commander will approve or disapprove the agency request for certification of vaults or secure rooms for open storage. In either case, a copy of the final package will be sent to the servicing ISPM, who will send it to the submitting agency. (The submitting agency will maintain the original for the life of the facility.)

5.20.7.6. (Added) When open storage is no longer required, the submitting agency will notify the servicing ISPM, in writing, that the vault or room is no longer being used for classified storage.

5.23.2. Personnel possessing the combination to a security container, vault, or secure room, will be listed on SF 700, **Security Container Information**. A continuation sheet may be used, but it must contain all the information required on SF 700.

5.23.4. (Added) Units are highly encouraged to permanently mark each security container (using an engraving tool) with the unit and security container number. The marking will be placed on either the top-front or left or right side-front of the security container. The purpose of this marking is to be able to positively identify security containers in the event of a disaster (fire, hurricane, or other natural disasters).

5.24.3. Refer to Federal Standard 809 (FED-STD-809), *Neutralization and Repair of GSA Approved Containers*, for additional information. Damaged or malfunctioning locks that do not meet Federal Specification FF-L-2740 will not be repaired; instead, new locks that meet this specification will be installed. **NOTE:** The combinations on all classified security containers will be reset to 50-25-50 before turn-in.

5.25. **Maintenance and Operating Instructions.** At least once per calendar year, safe custodians will perform a visual inspection of all classified security containers and annotate the results on AFTO Form 36, **Maintenance Record for Security Type Equipment**. Custodians will check for worn or damaged parts, loose handles, and other deficiencies that could degrade protection of the container.

5.26.3.1. AETC VA 31-5, *Classified Reproduction Authorized*, will be posted above or on all copiers approved for reproduction of classified material. AETC VA 31-6, *Unclassified Reproduction Only*, will be posted above or on all copiers, fax machines, and scanners not approved for reproduction of classified material.

5.27. **Control Procedures.** This information will be incorporated into local unit or staff agency security OIs.

5.28.2. During annual program reviews, ISPMs will review at least 25 percent of a unit's or staff agency's classified holdings and document the results in the report.

5.29.2.2. Two cleared persons must be involved in the destruction process—one destroying the material and one witnessing the destruction.

5.29.2.4. ISPMs are authorized to coordinate with the servicing medical facility to use medical incinerators for the destruction of classified CD-ROMs. Installations not equipped with medical incinerators may send CD-ROMs for destruction to the National Security Agency, 9800 Savage Road, ATTN: CMC-S 714, Suite 6890, Fort George G. Meade MD 20755-6000. **CAUTION:** Certain types of Sony® CD-ROMs may be toxic and, therefore, must not be incinerated.

5.29.2.5.1. (Added) AETC VA 31-7, *Classified Destruction Only*, will be posted on all shredders authorized for destruction of classified information.

5.29.2.5.2. (Added) AETC VA 31-8, *Unclassified Destruction Only*, will be posted on all shredders not authorized to destroy classified information.

6.2.1. Personnel will receive information from the local information assurance office about transmitting Secret, Confidential, and sensitive unclassified information via electronic means.

6.3.2. Procedures for receipting and safeguarding registered, certified, and first class mail and Federal Express packages will be included in unit and staff agency local OIs.

6.6.4.1. AF Form 310, **Document Receipt and Destruction Certificate**, will be used for this purpose.

6.9. **Handcarrying or Escorting Classified Material Aboard Commercial Passenger Aircraft.** The squadron commander or staff agency chief must sign the memorandum authorizing the handcarrying of classified material aboard commercial passenger aircraft.

8.3.7. (Added) Unit and staff agency security managers must complete localized training and L6AGU3P071-000 in accordance with paragraphs 1.3.5.2. through 1.3.5.2.2. (Added). Training must be documented and maintained in the security manager's handbook. Documentation may be maintained at other record-keeping locations (training records, office files, etc).

8.6. **Original Classification Authorities (OCAs).** HQ AETC/SFI will ensure original classification authorities (OCA) receive required training.

8.9.1.1. Together, professional security personnel and security managers will develop a local annual training plan (by calendar quarters) to ensure effective training of all assigned personnel. In addition, they will develop training to meet security education requirements that are commensurate with the needs of the personnel and unit mission.

8.11.2. Unit and staff agency local OIs will outline training responsibilities for supervisors and security managers.

8.15.2. The ISPM will document the effectiveness of the unit or staff agency security training program during the annual program review.

9.7. **Reporting and Notifications.** The unit inquiry officer will conduct preliminary inquiries of all incidents that do not involve the compromise of classified information. Preliminary inquiries will primarily focus on procedural and administrative errors or processes that resulted in a security deviation. Inquiries do not require sworn statements or other supporting documentation. The inquiry officer will answer the who, what, where, when, why, and how regarding the incident. If possible, he or she will identify the party

or parties responsible for the incident and recommend corrective actions to the appointing authority. If, during the preliminary inquiry, the officer establishes a compromise of information, the commander will initiate an investigation.

9.7.1.1. (Added) A person in the grade of MSgt, 2d Lt, GS-9, or higher will be appointed as the inquiry or investigative official, and a copy of the appointment memorandum will be provided to the servicing ISPM.

9.7.1.2. (Added) The unit security manager will notify the sending activity regarding the incident, complete a memorandum for record, and file it in the security manager's handbook.

9.7.1.3. (Added) A copy of all notifications, coordinations, etc., will be documented in the report of investigation.

9.8. **Preliminary Inquiry.** Before submitting the report to the appointing authority, the inquiry or investigative official will provide a draft of the report to the servicing ISPM for technical review.

9.8.1. The preliminary inquiry will be closed in 10 calendar days, unless the appointing authority grants an extension, in writing, to the inquiry or investigative official. In this case, the appointing authority will provide a copy of the extension to the ISPM. Extensions may only be granted for a total of 10 additional days. **NOTE:** The sample memorandum in Attachment 8 of the basic AFI indicates the preliminary inquiry will be closed in 30 days. In AETC, the inquiry will be closed in 10 calendar days unless an extension is granted (as indicated earlier in this paragraph).

9.9. **Damage Assessment.** Before submitting the report to the appointing authority, the inquiry or investigative official will provide a draft of the report to the servicing ISPM for technical review.

9.11.1. The appointing authority will concur or nonconcur with the inquiry or investigative report by first endorsement.

9.11.5. (Added) ISPMs will send HQ AETC/SFI any investigative report determined to be a compromise or potential compromise.

9.13. (Added) **Forms Adopted.** DoE Form 5631-20; SFs 312, 700, and 701; AFTO Form 36; and AF Forms 116, 310, 614, 673, and 1768.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Abbreviations and Acronyms

JPAS—Joint Personnel Adjudication System

OI—operating instruction

SK—sentinel key

JOHANN R. KINSEY, Colonel, USAF
Director of Security Forces