

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



**AIR FORCE INSTRUCTION 31-401
AIR EDUCATION AND TRAINING COMMAND
Supplement 1
14 SEPTEMBER 1999**

Security

**INFORMATION MANAGEMENT SECURITY
PROGRAM**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO/PP WWW site at:
<http://afpubs.hq.af.mil>

OPR: HQ AETC/SFI (MSgt J. Schell)
Supersedes AFI 31-401/AETC Sup 1, 31 March
1995

Certified by: HQ AETC/SF (Mr H. Beavers)
Pages: 7
Distribution: F; X: HQ USAF/XOFI - 1

"HOLDOVER"

*"The basic publication has changed; impact on supplemental information is under review
by the OPR. Users should follow supplemental information that remains unaffected."*

AFI 31-401, 1 January 1999, is supplemented as follows and will be used in conjunction with DoD 5200.1-R, *Information Security Program*, and DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*:

NOTES:

1. 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.
2. Maintain and dispose of records created as a result of processes prescribed in this publication in accordance with AFMAN 37-139, *Records Disposition Schedule*.
- 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 non-AETC units on AETC installations, in writing, 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 participate fully in the host-base information security program.
- 1.3.5.1. Unit commanders or staff agency chiefs appoint a primary security manager and as many alternates as necessary. Provide a copy of the appointment memorandum to the ISPM.

1.3.5.2. All newly assigned security managers and alternates will notify the ISPM within 15 days of assignment to be scheduled for security manager's training. Security managers and alternates must be trained within 90 days of appointment.

1.3.6.2. Route draft copies of proposed or revised unit security operating instructions through the servicing ISPM via AF Form 673, **Request to Issue Publication**, for coordination prior to publication. Provide a final copy of the operating instruction to the ISPM.

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

1.3.6.9.1. Section 1, commander's appointment memorandum.

1.3.6.9.2. Section 2, security manager training certificates.

1.3.6.9.3. Section 3, most recent annual program review from the ISPM.

1.3.6.9.4. Section 4, last two semiannual security self-inspections, with appointment memorandums for the inspecting officials.

1.3.6.9.5. Section 5, unit security operating instruction.

1.3.6.9.6. Section 6, training section, containing training materials used for in-processing and recurring training. This section will also contain validation of training accomplishment.

1.3.6.9.7. Section 7, Automated Security Clearance Access System (ASCAS) or Sentinel Key security data.

1.3.6.9.8. Section 8, information or policy memorandums. Retain according to the appropriate table and rule in AFMAN 37-139. File the last two semiannual security manager's meeting minutes in this section.

1.3.6.9.9. Section 9, if applicable, copies of vault or secure room certification.

1.3.6.9.10. Section 10, if applicable, industrial security contracts and related correspondence.

1.3.6.9.11. Section 11, miscellaneous items.

1.4.1. Unit security management and information security oversight requirements are 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 the above measurements, or combining any two of the above measurements, 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 do not conduct these inspections.

1.4.3.2. (Added) Unit commanders and staff agency chiefs designate personnel, in writing, to conduct semiannual security inspections of their activities for regulatory compliance. HQ AETC/SFI prepares and distributes checklists to ISPMs. ISPMs are strongly encouraged to localize the checklist. Unit commanders and staff agency chiefs provide a copy of the semiannual security inspection report to the servicing ISPM along with a copy of the appointment memorandum.

NOTE: Program reviews conducted by ISPMs may count as one of the unit 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 (DoE Form 5631-20, **Request for Visit or Access Approval**), including critical nuclear weapon design information (CNWDI) material in the hands of Department of Energy (DoE) or federal agencies other than the National Aeronautical and Space Administration: (**NOTE:** This authority can not be delegated further.)

1.5.1.1.2.1. Installation commanders.

1.5.1.1.2.2. Commanders of the 363d Training Squadron and 365th Training Squadron, Sheppard AFB; 37th Civil Engineer Squadron (CES), Lackland AFB; 56th CES, Luke AFB; 325th CES, Tyndall AFB; 343d and 342d Technical Training Squadron, Lackland AFB; Det 2, 366th Training Squadron, Indian Head NSWC; and Det 3, 366th Training Squadron, Eglin AFB.

1.5.1.1.2.3. Chief, Technical Training Division, HQ AETC Directorate of Operations (HQ AETC/DOO).

1.7.2. 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 original classification authorities (OCA) up to and including Secret: Commander, AETC (AETC/CC); Director of Logistics (HQ AETC/LG); and Commander, Air University (AU/CC).

2.3.2. Send an information copy to HQ AETC/SFI.

4.8. (Added) Marking Notebooks, Binders, and Similar Holders. Mark notebooks, binders, etc., containing classified information conspicuously with the highest classification of the material contained. Affix the appropriate classified cover sheet to the front and back of the binder, notebook, or holder. Also mark the spine on binders, notebooks, or holders with the overall classification.

4.9. (Added) Envelopes, File Folders, and Dividers in Classified Safes. Mark envelopes in classified storage containers containing classified documents on the front and back with the highest classification maintained. Mark the tops and bottoms of file folders and dividers with the highest level of classification maintained in that record series.

5.4.2. (Added) Security Access Requirement (SAR) Coded Positions. Any person having access to classified material, information, or briefings three or more times during a calendar month will be in a SAR coded position. The position will be coded to reflect the appropriate access level (Secret, Top Secret, or SCI) on the unit manning document. Coordinate any additions or deletions of unit or staff agency SAR codes through the host ISPM before processing through the local manpower office.

5.5.4. (Added) Attesting to Security Commitment. All military and civilian personnel with Top Secret access and or who have access to special access program material (Top Secret, Secret, Confidential) or sensitive compartmented information must orally attest to their security commitment. Contractors are not included at this time. Use the following procedures:

5.5.4.1. 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. Individuals completing the SF 312 for the first time, and assigned to a Top Secret or special access position, will complete the security attestation when they read and sign the SF 312.

5.5.4.3. Two people must witness all attestations. Record in a memorandum the name of the person making the attestation and have the person acknowledge receipt by endorsement. Both witnesses will also

endorse the memorandum. Unit or staff agency security managers must maintain the documentation. Provide a copy to the person making the attestation to show as proof for future assignments or accesses.

5.10.1.1. Provide a copy of the Top Secret Control Officer (TSCO) appointment memorandum to the servicing ISPM.

5.10.1.3.1. Provide a copy of the annual inventory report to the servicing ISPM.

5.12. Incorporate end-of-day security check procedures into activity operating instructions. The 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, both physically and against sound emissions. Establish entry control and perimeter surveillance by posting personnel from the sponsoring activity in and around the room or facility as necessary. Security Forces are not responsible for this function but may assist in the review of unit security plans.

5.17.1. Incorporate unit or staff agency certification procedures for classified information processing equipment into unit security operating instructions.

5.17.2.1. During annual program reviews, ISPMs will ensure all computer systems designated for the processing of classified information are accredited and a current risk analysis is on file.

5.20.3. All GSA security containers and doors used to store classified material will be retrofitted with locks meeting Federal Specification FF-L-2740 by FY 2005. The only existing lock that currently meets the federal specifications is the XO-7 by MAS Hamilton.

5.20.3.1. (Added) All security containers used for storing Top Secret or special access material will be equipped with locks meeting Federal Specification FF-L-2740.

5.20.3.2. (Added) All open storage areas, secure rooms, and vaults will be equipped with locks meeting Federal Specification FF-L-2740, unless waived by HQ AETC/SF. Process waiver requests through normal command channels. The AF Form 116, **Request for Deviation from Security Criteria**, may be used.

5.20.4. (Added) Storing Classified Material for Other Units or Staff Agencies. AETC units or staff agencies may store classified material for other units or staff agencies when the volume of classified material, or frequency of use, does not justify maintaining a security container. Place the material in a sealed envelope or a sealed container; mark the envelope or container front and back with the highest classification. The owning agency provides the storing agency a memorandum listing names, organizational addresses, telephone numbers, and security clearances of personnel authorized access to the envelope or container. The owning agency reviews the material quarterly. The reviewing official dates and signs a review sheet/log attesting the material is still required. Use AF Form 614, **Charge Out Record**, when the material is temporarily removed. Establish procedures to ensure all classified material is returned to the storage container before the end-of-day check.

5.20.5. (Added) Vaults and Secure Rooms. The structural standards identified in DoD 5200.1-R, Appendix G, and Military Handbook 1013/1A, apply to AETC activities. Vaults and secure rooms previously certified and approved before January 1997 are still valid and do not require recertification. Tenant units on AETC installations that participate in the host base information security program will follow these procedures. If tenant units do not participate in AETC information security programs, they will follow their MAJCOM's guidance, a copy of which will be provided to the host ISPM. The following guidance applies:

5.20.5.1. AETC activities should consider building a secure room to store Secret and Confidential materials when mission needs dictate these types of facilities are necessary. These structures will provide an effective safeguarding capability and eliminate the high costs associated with building vaults.

5.20.5.2. Compensatory measures are required when vaults or secure rooms do not meet the construction standards in DoD 5200.1-R, Appendix G, and Military Handbook 1013/1A. Compensatory measures must be applied before open storage of classified material may be approved. Refer to DoD 5200.1-R, 6-402, for supplementary controls involving storage of Top Secret material.

5.20.5.3. Modifications made to vaults and secure rooms rescind any previous certification and approval authority for continued open storage of classified materials. Use the guidelines in DoD 5200.1-R, Appendix G. The ISPM and Civil Engineer must recertify the structural integrity of vaults and secure rooms even if they were previously built to standards.

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

5.20.6.1. The ISPM and Civil Engineer reviews all new construction or structural modifications, before construction or before compensatory measures are included, 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, if the facility does or does not meet physical security standards. The unit or staff agency submits a written plan or operating instruction outlining procedures for providing protection and positive entry control to the vault or secure room. The ISPM will certify the plan or operating instruction provides adequate safeguards for the protection of classified material. If the facility meets standards, no further action is required. If the facility does not meet structural standards, the following will be accomplished:

5.20.6.1.1. The unit or staff agency submits its written plan to the installation commander, through the ISPM and Civil Engineer, via AF Form 1768, **Staff Summary Sheet**. The package will contain applicable compensatory measures for the level of certification required--Secret or Top Secret. In-depth security will be addressed along with completing a risk analysis. Attach copies of the ISPM and Civil Engineer physical security reviews. Enclose floor plans of the facility. The ISPM and Civil Engineer will concur or non-concur with the request. If the ISPM or Civil Engineer nonconcur, he or she will provide rationale for the decision and attach it to the package.

5.20.6.1.2. The installation commander will approve or disapprove the agency request for certification of vaults or secure rooms for open storage. If approved, provide a copy of the final package to the servicing ISPM. The submitting agency will maintain the original for the life of the facility.

5.20.6.1.3. When open storage is no longer required, the unit or staff agency must notify the servicing ISPM, in writing, that the vault or room is no longer used for classified storage.

5.23.2. List all personnel possessing the combination to a security container, vault, or secure room on SF 700, **Security Container Information**. You may use a continuation sheet, but it must contain all the information required on SF 700.

5.24.4. (Added) Refer to Federal Standard 809 (FTD-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 must not be repaired. Install new locks meeting FF-L-2740 standards.

5.24.5. (Added) Reset the combinations on all classified security containers to 50-25-50 before turn-in.

- 5.25. 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 the protection standards of the container.
- 5.27. Incorporate this information into local unit or staff agency security operating instructions.
- 5.28.2. During annual program reviews, ISPMs will review, at a minimum, 25 percent of a unit's or staff agency's classified holdings. Program managers will document 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, Maryland 20755-6000. **CAUTION:** Certain types of Sony CD-ROMs may be toxic and can not be incinerated.
- 6.2.1. Personnel will receive information about transmitting Secret, Confidential, and Sensitive Unclassified information via electronic means from the local Information Assurance Office.
- 6.3.2. Include procedures for receipting and safeguarding registered, certified, first class mail, and Federal Express packages in unit and staff agency local operating instructions.
- 6.6.4.1. Use AF Form 310, **Document Receipt and Destruction Certificate**, for this purpose.
- 6.9. The squadron commander or staff agency chief must sign the memorandum authorizing the handcarrying of classified material aboard commercial passenger aircraft.
- 8.3.1. Unit and staff agency security managers ensure training is provided within 30 days of assignment and that the training is documented.
- 8.4. Unit and staff agency security managers ensure training is provided within 30 days of assignment and that the training is documented.
- 8.5. HQ AETC/SFI will ensure OCAs receive required training.
- 8.9.1. (Added) Develop a local annual training plan (by calendar quarters) to ensure effective training of all assigned personnel. Develop training to meet security education requirements that are commensurate with the needs of the personnel and unit mission.
- 8.9.2. (Added) Unit and staff agency local operating instructions must outline training responsibilities for supervisors and security managers.
- 8.12. ISPMs document the effectiveness of the unit or staff agency security training program in the annual program review.
- 9.3.2.1. The inquiry/investigative official will be a person in the grade of MSgt, 2d Lt, GS-9, or higher. Provide a copy of the appointment memorandum to the servicing ISPM.
- 9.3.2.2. Unit security managers notify the sending activity regarding the incident and complete a memorandum for record and file it in the security manager's handbook.
- 9.3.2.3. Document this coordination in the report of investigation.

9.3.2.4. (Added) Prepare a report of inquiry/investigation using the following format in conjunction with AFI 90-301, *Inspector General Complaints*. The report consists of seven main sections as follows:

9.3.2.4.1. Authority. This section cites the authority for conducting the inquiry and identifies the inquiry/investigation official.

9.3.2.4.2. Matters Investigated. This section contains a brief statement of the circumstances surrounding the incident, the location of the incident, how the incident was initially discovered, and what type of classified material was involved.

9.3.2.4.3. Personnel Interviewed. Identify all personnel who were interviewed by grade, full name, phone number, and organizational address.

9.3.2.4.4. Findings. In chronological order, present all facts as derived from the testimony of personnel interviewed. This section should contain a brief summation from every person interviewed who provided relevant information. Attempt to corroborate and validate findings.

9.3.2.4.5. Conclusion. State the category of the incident as either a security deviation or compromise. Identify the party or parties responsible for the infraction and how this conclusion was developed.

9.3.2.4.6. Recommendations. Based on the conclusion, the inquiry/investigative officer recommends the incident be closed as either a security deviation or compromise. This section should also be used to refer the investigation to another agency if the inquiry/investigative official determines criminal elements are involved. The inquiry/investigative official should identify corrective actions to prevent future incidents.

9.3.2.5. (Added) The inquiry/investigative official provides a draft of the report to the servicing ISPM for technical review before submitting the report to the appointing authority.

9.3.3. (Added) Preliminary Inquiries:

9.3.3.1. Conduct preliminary inquiries for all incidents that do not involve the compromise of classified information. If during the preliminary inquiry, you establish the compromise of information, initiate an investigation. Preliminary inquiries 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, identify the party or parties responsible for the incident and recommend corrective actions to the appointing authority.

9.3.3.2. Close preliminary inquiries in 10 calendar days, unless the appointing authority grants an extension, in writing, to the inquiry officer. 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.

9.4.1.4. The appointing authority must concur or nonconcur with the inquiry/investigative report by first endorsement.

9.6.1.4. (Added) ISPMs will forward all investigative reports to HQ AETC/SFI deemed to be a compromise or potential compromise.

RICHARD K. ELDARD, Colonel, USAF
Director of Security Forces