

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 before publication. Provide a final copy of the operating instruction to the ISPM.

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

1.3.6.9.1. (Added (MAFB). Section 1, Commander's appointment memorandum

1.3.6.9.2. (Added (MAFB). Section 2, Security Manager's training certificates

1.3.6.9.3. (Added (MAFB). Section 3, Most recent annual program review from the ISPM

1.3.6.9.4. (Added (MAFB). Section 4, Last two semiannual security self-inspections, with appointment memorandums for the inspecting officials

1.3.6.9.5. (Added (MAFB). Section 5, Unit security operating instruction

1.3.6.9.6. (Added (MAFB). Section 6, Training section, containing training materials used for in-processing and recurring training. This section also contains validation of training accomplishment

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

1.3.6.9.8. (Added (MAFB). 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. (Added (MAFB). Section 9, If applicable, copies of vault or secure room certification

1.3.6.9.10. (Added (MAFB). Section 10, If applicable, Industrial security contracts and related correspondence

1.3.6.9.11. (Added (MAFB). Section 11, Miscellaneous items

1.4.3.2. (Added (MAFB) 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.

4.8. (Added (MAFB). **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 (MAFB). **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 (MAFB). **Security Access Requirements (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. **NOTE: The unit commander must sign SAR letters.**

5.5.4. (Added (MAFB). **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 read paragraph 1 of the SF 312, **Classified Information Nondisclosure Agreement**, and verbally state they understand it and abide, without equivocation, by its direction.

5.5.4.2. (Added (MAFB). Individuals completing the SF 312 for the first time, and assigned to a Top Secret or special access position, complete the security attestation when they read and sign the SF 312.

5.5.4.3. (Added (MAFB). 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 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.

5.17.1. 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 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 are 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 (MAFB). 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 (MAFB). All open storage areas, secure rooms and vaults are 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 (MAFB). **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 (MAFB). **Vaults and Secure Rooms.** The structural standards identified in DOD 5200.1-R, Appendix G and Military Handbook 1013/1A apply to AETC activities. Vault 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 follow their MAJCOMs guidance, a copy of which is provided to the host ISPM. The following guidance applies:

5.20.5.1. (Added (MAFB). 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 provide an effective safeguarding capability and eliminate the high costs associated with building vaults.

5.20.5.2. (Added (MAFB). 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. (Added (MAFB). 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 (MAFB). **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. (Added (MAFB). 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 certifies, 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 certifies 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 is accomplished:

5.20.6.1.1. (Added (MAFB). 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 contains applicable compensatory measures for the level of certification required—Secret or Top Secret. In-depth security is 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 concur or nonconcur with the request. If the ISPM or Civil Engineer nonconcur, he or she provides rationale for the decision and attach it to the package.

5.20.6.1.2. (Added (MAFB). The installation commander approves or disapproves 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 maintains the original for the life of the facility.

5.20.6.1.3. (Added (MAFB). When open storage is no longer required, the unit or staff agency notifies the servicing ISPM, in writing, that the vault or room is no longer 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 (MAFB). 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 (MAFB). Reset the combinations on all classified security containers to 50-25-50 before turn-in.

5.25. Once per calendar year, safe custodians perform a visual inspection of all classified security containers and annotate the results on AFTO Form 36, **Maintenance Record for Security Type Equipment**. Custodians 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 review, at a minimum, 25 percent of a unit's or staff agency's classified holding. Program managers document results in the report.

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 cannot be incinerated.

6.2.1. Personnel receive information about transmitting Secret, Confidential, and Sensitive Unclassified information via electronic means from the local Information Assurance Office.

6.2.3. Include procedures for receipting and safeguarding registered, certified, first class mail and Federal Express packages in unit and staff agency local operating instructions.

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.

8.9.1. (Added (MAFB). 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 (MAFB). 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 training program in the annual/biennial program review.

9.3.2.1. The inquiry/investigative official is 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 (MAFB). 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.

REX E. OGLE, Jr., Maj, USAF
Commander, Security Forces Squadron