



**MANAGING THE INFORMATION 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: 375 SFS/SFAI (Ms. Morris)
Supersedes AFI 31-401/SAFB1, 29 Aug 1997

Certified by: 375 SFS/SFAI (Mr. Martinusen)
Pages: 5
Distribution: F

AFI 31-401, 1 January 1999, is supplemented as follows:

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.

1.3.5.1. Unit commanders or staff agency chiefs appoint a primary security manager and as many alternates as necessary. Provide the original of the appointment memorandum to the Information Security Program Manager (ISPM). Maintain a copy of this memorandum in the Security Manager's Handbook.

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

1.3.6.4. Security manager meetings will be held semiannually in March and September each year. All security managers from units or staff agencies within the 375 AW must attend the semiannual security managers' meeting. If the primary or alternate cannot attend, a suitable substitute must attend. Security managers from tenant units or staff agencies, as well as contractors and long-time visitors, are encouraged to attend.

1.3.6.9. (Added) Maintain a Security Manager's Handbook containing, at a minimum, the following items:

1.3.6.9.1. Section 1. Commander's appointment memorandum, security manager training certificates and memorandums, and a memorandum on classified safes and locations, if applicable.

1.3.6.9.2. Section 2. Internal Security Operating Instructions. These do not have to be done annually, as long as the information is still current.

1.3.6.9.3. Section 3. Semiannual Security Inspection Reports. Keep the last two semiannual security self-inspections, along with the appointment memorandum. The commander must appoint an individual other than the security manager to conduct the self-inspections.

1.3.6.9.4. Section 4. Information Security Program Review Reports. Keep the last two program review reports from the ISPM.

1.3.6.9.5. Section 5. Security Manager's Meeting Minutes. Keep the last two semiannual security manager's meeting minutes in this section.

1.3.6.9.6. Section 6. Information Memorandums. Keep information memorandums for the last year.

1.3.6.9.7. Section 7. Automated Security Clearance Approval System (ASCAS) Rosters (both military and civilian) or Sentinel Key security data.

1.3.6.9.8. Section 8. Miscellaneous Items. Keep the log sheets on the Attestations of the Standard Form 312, **Classified Information Nondisclosure Agreement**, and any posters, etc., in this section.

1.3.6.9.9. Section 9. Training Plan. Maintain your annual training plan and all documentation in this section. This section is also used for training materials used for in-processing and any recurring training.

1.4.2. The ISPMs will retain the last two annual program reviews in the management folders.

1.4.3.1. If the program review is conducted in January or July, the ISPM may count the annual program review as one of the semiannual self-inspections.

2.1. There is no original classification authority within the 375 AW.

2.5. (Added) Coordinate all classified wing plans through Security Forces Information Security (375 SFS/SFAI) for proper classification markings.

4.1. Warning notices shall be placed on file folders, binders and storage media; same as for classification markings.

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.

4.9. (Added) Envelopes and File Folders in Classified Safes. Mark envelopes in classified storage containers containing classified documents on the front and back with the highest classification maintained. Mark the top and bottom of the file folders and labels with the highest level of classification maintained in that folder.

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. Send a SAR-code memorandum to the host ISPM for any additions or deletions of unit or staff agency SAR codes for approval.

5.5. Maintain a copy of the Standard Form 312 in the Security Manager's Handbook until the Automated Security Clearance Approval System (ASCAS) Roster/Sentinel Key reflects the individual has signed the Standard Form 312.

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. The attestation must be documented on an AF Form 2583, **Request for Personnel Security Action**, Section VII, Item 30, which is the "Remarks Section" of the form: EXAMPLE: "Attestation com-

pleted on (ENTER DATE).” Also, annotate all individuals who have completed the attestation on a Log Sheet to be kept in the Security Manager’s Handbook under Section 8.

5.5.4.2. Individuals in Top Secret or special access positions will read paragraph 1 of the Standard Form 312 and verbally state they understand it and will abide, without equivocation, by its direction.

5.5.4.3. Individuals completing the Standard Form 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 Standard Form 312.

5.5.4.4. 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 in Section 8 of the Security Manager’s Handbook. Provide a copy to the person making the attestation to show as proof for future assignments or accesses.

5.10.1.1. Within 375 AW send the appointment memorandum to 375 SFS/SFAI.

5.12. Standard Form 702, **Security Container Check Sheet**, shall be located on the top of the classified storage container. The Standard Form 701, **Activity Security Checklist**, is not required in areas that are continuously staffed.

5.14. Transient personnel arriving or departing after normal duty hours may secure storage of classified material in their possession through the Senior Controller, Scott Command Post, 375 AW/CP, Bldg 505. Material will be securely fastened so evidence of tampering can be easily detected. The package should be double-sealed in an opaque container and marked with the name and phone number of the person dropping off the package, to include an AF Form 310, **Document Receipt and Destruction Certificate**.

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.

5.19. Storage containers for classified material will be numbered by functional address symbol (FAS) and by number (XX-1, XX-2, etc.). The security manager will maintain a list of storage container designations with serial numbers, make, and model of container showing exact location of the safe (FAS, building/room number). Emergency plans will be posted on the outside of the classified storage containers.

5.20.4. (Added) Storing Classified Material for Other Units or Staff Agencies. The 375 AW 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 number, 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 an 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 DODD 5200.1, DOD Information Security Program, Appendix G, apply to 375 AW activities.

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 375th Civil Engineer reviews all new constructions or structural modifications before construction or compensatory measures are included, to ensure the vault or secure room design meets physical security standards for Secret or Top Secret storage. A memorandum from the unit requesting an inspection will suffice. Once construction or modifications are complete, the ISPM and 375th 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 ensuring adequate safeguards for the protection of classified material. If the facility meets standards, no further action is required. Both the unit and the ISPM will keep a copy of the certification.

NOTE: The definition of open storage is material which cannot be stored in a security container due to its bulk and the facility does not meet the criteria of a vault.

5.25. Each time a combination is changed, safe custodians will perform a visual inspection of the classified security container. Custodians will check for worn or damaged parts, loose handles, and other deficiencies that could degrade the protection standards of the container.

5.29. Unit or agencies on Scott AFB may call 375 CSS/SCCBS, Document Security Section, 256-3054/4340, for appointments to destroy classified material consisting of paper products, typewriter ribbons, plastic tapes, and viewgraph slides. Typewriter ribbons, plastic tapes, and viewgraph slides must be intermingled with paper when destroying this material. (For further guidance, refer to SAFBI 37-101, **Access and Use of the Base Destruction Facility**.) Individuals requiring use of degaussing equipment must contact the Computer Operations Library Branch, 256-2650.

6.2.3. Unit commanders or staff agency chiefs will report denial or revocation of clearance of personnel designated as classified message or document couriers for any reason. This could include the Document Security Section, Base Communications Center, the base COMSEC Account, 256-4057, Command Post, Wing Plans, etc.

6.2.4. (Added) The Document Security Section personnel are authorized to open the inner wrappers of classified items insufficiently addressed to Scott AFB agencies to determine direct distribution. (**EXCEPTION:** Items addressed to base COMSEC, 375 CSS/SCCC, or CA6XXXXX (XXXXX = any other number)—items with either of these addresses will not be opened. Call 256-4057 for pick up.)

6.8. NOTE : Purpose of this requirement---All units are under the purview of the 375 AW/CC. The DD Form 2501 is not issued to individuals who hand-carry or escort classified material on the installation when they are not expected to pass through an inspection point. The DD Form 2501 is issued to individuals who hand-carry or escort classified material when they are expected to pass through an inspection point or leave the installation (this refers to the local Metro East area only). If this applies, procedures should require storage of the DD Forms 2501 within the authorizing activity's files during all periods when the authorized individual is off duty and not involved with hand-carry or escort of classified material. Individuals who serve in an "on-call" capacity, such as Duty Officer, may be considered on duty. DD Forms 2501 will be issued with a specific expiration date of not more than 1 year from the date of issue. Whenever the authorized individual is no longer assigned to or employed by the issuing organization, the

respective DD Form 2501 is invalidated and retained in the issuing organization's files for an additional 2 years before destruction. Classified material hand-carried outside a facility must be in an envelope, folder or other closed container to prevent loss or observation that classified material is being hand-carried. (Optional Form 65-B, **U.S. Government Messenger Envelope**, is not considered a closed container.) An appropriate classified cover sheet can be used when hand-carrying material between different unit or agencies within the same building. **NOTE:** The authorization for hand-carrying or escorting classified material outside the local area consists of an approved courier letter and an exemption notice affixed to the package containing classified.

8.1. Annual training will be developed and broken down into calendar quarters. A roster must be prepared and maintained showing training conducted and dates of individuals trained.

8.9.1. (Added) All security managers from units or staff agencies on this base who have contract personnel assigned will complete Category II training on these contract personnel.

9.2. All security incidents for the wing and tenant units participating in the wing program must be reported by telephone within the first duty day to 375 SFS/SFAI, 256-5403. In cases of improper transmission of classified material, the sending activity is responsible for conducting the preliminary inquiry.

STANLEY J. MCCLOSKEY, Lt Col, USAF
Commander, 375th Security Forces