



**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 AFRC/SFI (Ms Kathy Simonton)

Certified by: HQ AFRC/SF  
(Col Michael E. Swaney)

Supersedes AFI 31-401, 1 January 1999, and  
AFI 31-401/AFRC Sup, 1 July 1999

Pages: 26  
Distribution: F

---

This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-401, 1 November 2001. The AFI is published word-for-word without editorial review. Air Force Reserve Command supplementary material is indicated by “(AFRC)” in boldface type. This supplement describes Air Force Reserve Command procedures to be used in conjunction with the basic instruction. Upon receipt of this integrated supplement discard the Air Force basic.

**SUMMARY OF REVISIONS**

This revision is necessary to align paragraphs and attachments. This revision explains who the ISPM is and responsibilities (para **1.3.4.**); makes attendance at security managers meetings mandatory (para **1.3.6.4.**); clarifies program review requirements (para **1.4.2.**); provides instructions on authorized system for retrieving security clearance information (para **5.4.1.1. (Added)**); clarifies the correct address to send NdAs for reservists and IMAs (para **5.5.1.2.**); outlines procedures when hosting classified meetings (para **5.15.2.**); lists electronic devices unauthorized in areas that transmit classified (para **5.15.6. (Added)**); identifies visual aids to be used at all machines approved for classified reproduction (para **5.17.1.**); expands procedures for secure storage rooms (para **5.20.5. (Added)**); makes approval for areas using key-operated locks to store classified mandatory (para **5.21.1.**); ensures lock and key custodians are cleared (para **5.21.2.**); requires control of keys (para **5.21.3. (Added)**); gives information on approved destruction devices (para 5.29.1.4.); identifies timeline for appointment of inquiry official (para **9.8.1.**); details inquiry report requirements (para **9.8.2.**). A bar (|) indicates changes from the previous edition.

1.3.3.3. The Director of Security Forces, HQ AFRC, formulates, disseminates, and interprets policy in this supplement.

1.3.4. The Director of Security Forces (HQ AFRC/SF) is the command Information Security Program Manager (ISPM). Main operating base ISPMs are responsible for ensuring supported Geographically

Separated Units (GSU), Sites and Activities comply with this program. The Numbered Air Forces (NAF) staff and their associated units fall under their host base ISPM. NAFs are also responsible for ensuring contingency sites and locations under their control comply with this program.

1.3.4.4. (Added) Information Security Program Managers (ISPM) conducts security manager meetings as needed.

1.3.5.1. Appoint as the primary security manager a full time employee of the organization. Due to the importance of security manager duties, commanders/directors must refrain from assigning further additional duties to individuals performing security manager duties. Provide the ISPM a letter of appointment of a primary and alternate security manager.

1.3.6.1. Maintain a security manager’s handbook with the following: Security manager letter of appointment, internal security operating instructions, semiannual security self-inspection reports for last two years, security manager meetings minutes, information letters, inspection checklists, program review report, signed annual training plan and list of security containers, vaults, and secure rooms located in the organization.

1.3.6.4. Mandatory attendance at ISPM hosted security manager meetings is required by primary or alternate security manager.

1.4.1. HQ AFRC/SFI conducts Information Security Program Oversight Visits (ISPOVs) at AFRC installations every two years or in conjunction with Staff Assistance Visits (SAVs). ISPMs assist in the ISPOV.

1.4.2. ISPOVs are assistance-orientated visits to identify noteworthy and problem areas in the Information, Personnel, Industrial, and NATO Security Programs. They must be extensive enough to determine overall status of the program and must include an assessment of the security education and training as a special interest item. Replies to ISPOV reports are generally not required; however, corrective action(s) taken to correct identified problem areas should be recorded.

1.4.3. All units will conduct semiannual security self-inspections, one between 1 January and 30 June, and one between 1 July and 31 December. Program Reviews can substitute for one of the semiannual security self-inspections if identified in the program review report. Units with a small volume of classified (25 documents or less) or no classified may conduct an annual self-inspection.

1.4.3.1. A knowledgeable person must be assigned to conduct self-inspections. Security Managers will not conduct self-inspections within their own directorate/unit; however, they are normally the most qualified individuals to inspect programs outside their directorate/unit and commanders/staff agency chiefs are encouraged to utilize them in that role.

1.5.1.1. The following officials may grant access to Restricted Data: HQ AFRC/CV and 2-Ltr staff agency chiefs at HQ AFRC, and Wing Commanders.

1.6.1. HQ AFRC/SF may approve or disapprove waivers.

2.1.1. Original Classification Authority (OCA) designations are:

Commander, HQ AFRC	Top Secret
Vice Commander, HQ AFRC	Secret
Asst. Vice Commander	Secret
AFRC Numbered Air Forces/CC	Secret

Commander, Air Reserve Personnel Center      Secret

4.9. (Added) Holders must notify originator of improperly marked documents in writing, or record with a memo any telephonic notification. Notification must be kept with the document.

4.10. (Added) All binders that contain classified information will be marked on the spine with the highest level of classified stored therein. Exceptions would be binders that are too small to have an adequate spine.

5.4. For the purpose of granting access, the access level equates to clearance eligibility.

5.4.1.1. (Added) Do not use PCIII or Automated Security Clearance Approval System (ASCAS) roster. Only Sentinel Key or JPAS will be utilized to verify an individual's access level.

5.5. In absence of verification of signed NdA, complete new form and forward a copy to appropriate agency.

5.5.1.2. NdAs for reservists and IMAs are sent to: HQ AFRPC/DPBA, 6760, East Irvington Place, Denver, CO 80280

5.7.1.1. ISPMs may forward visit request in the absence of security managers. Ensure the local contracting office receives a copy of the visit request.

5.10.1. See [Attachment 17 \(Added\)](#) for Top Secret Control Guidance.

5.10.1.1. ISPMs provide training to newly appointed TSCOs.

5.10.2. Implement a documented accountability system (such as an inventory sheet) for Secret material retained over 30 days and stored in a GSA approved security container not located in a secure environment. The ISPM determines what constitutes a secure environment. Use an unclassified description of the material and file separately from the classified material. This will facilitate an assessment of a compromise.

5.11. Use AF Form 614, *Charge Out Record*, or similar form, when a document is removed from a security container.

5.11.3. (Added) Develop plans for the protection, removal, or destruction of classified material in case of natural disaster, fire, civil disturbance, terrorist activities, or enemy action. (DoD 5200.1-R, para 6-303). Include in your unit operating instruction (see sample at Attachment 7).

5.12. Each unit and staff agency which stores and processes classified information, do not have to use SF 701, *Activity Security Checklist*, or SF 702, *Security Container Check Sheet*, on security containers, vaults, or secure storage rooms where classified material is stored or handled when manned by cleared personnel on a 24-hour, 7-day-a-week basis. At no time under these conditions may the above be left unattended when opened.

5.12.1. (Added) Include on your SF 701 (if applicable): Check all classified computers to ensure that the hard drive has been removed and locked in a GSA approved container. Check all Global Command and Control System (GCCS)/SIPRNET connections to ensure they have been disconnected and properly locked away.

5.13.2. Within AFRC, removing classified information/material from designated work areas for work at home is prohibited.

5.14. AFRC installations must include designated overnight repository in their base supplement.

5.15.2. Installation commanders can delegate this authority in writing to the ISPM. The following procedures must be accomplished when hosting classified meetings:

5.15.2.1. (Added) Verify security clearances on attendees prior to any classified briefings or discussions.

5.15.2.2. (Added) Ensure the door to the discussion area is closed and someone is posted outside the door if sound attenuation and unauthorized entry is not adequate and cannot be controlled.

5.15.2.3. (Added) Ensure the briefing is kept to need-to-know for those in attendance.

5.15.2.4. (Added) Ensure classified is kept under constant surveillance. Use of classified cover sheets is required when material is removed from secure storage.

5.15.2.5. (Added) Return all classified material to secure storage when not under personal observation and control.

5.15.2.6. (Added) Note taking or electronic recording during classified sessions shall be permitted only when it is determined by the host that such action is necessary to fulfill the U.S. Government purpose for the meeting.

5.15.2.7. (Added) Classified waste must be destroyed using approved methods (burning, melting, pulping, pulverizing, and cross-cut shredding).

5.15.2.8. (Added) Ensure that classified documents, recordings, audiovisual material, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as required by this instruction and DoD 5200.1-R. **Information Security Program.**

5.15.6. (Added) Cellular phones, two-way radios, two-way beepers, and other electronic equipment that can receive and transmit a signal are prohibited in all offices and areas where classified and sensitive information may be discussed. Staff directors, NAF commanders, and wing commanders will determine which work areas are affected and implement this requirement accordingly. Owners of designated areas should make every effort to inform personnel of the prohibited use of electronic equipment, to include but not limited to posting signs and visual aids, and including the information in briefings and training, etc.

5.16. This paragraph was included in its entirety in Attachment 12 of IC-2002-2, 15 Dec 00.

5.17.1. Post visual aids at all machines (to include fax machines) approved for classified reproduction. At a minimum, post visual aids at all copy machines not authorized for classified reproduction. AFRCVA 31-404, **Classified Reproduction Rules**, and AFRCVA 31-405, **STOP Do not use this machine for classified Reproduction STOP**, should be used. These visual aids may be obtained from the AFRC Publications web site.

5.20. Security managers will develop and maintain a list of security containers, vaults, and secure rooms located in their organization and include in their security manager's handbook. This list will include make, ID number, lock type, and location.

5.20.1. Secure storage rooms containing open stored classified material, equipment or hardware built after 1 October 1995 must have an intrusion detection alarm operating when appropriately cleared attendants are not present. ISPMs determine whether open or unattended storage areas provide adequate protection for classified material. If "security-in-depth" practices are used in lieu of alarms, the MAJCOM ISPM must grant approval. Examples of "security-in-depth" are: use of perimeter fences, employee and visitor access controls, use of an IDS, random guard patrols throughout the facility during non-working

hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

5.20.3. ISPM must send requests to waive any provisions of DoD 5200.1-R and AFI 31-401 to HQ AFRC/SF for concurrence.

5.20.3.1. (Added) Post the storage facility approval notices/letters inside the approved area.

5.20.4. FF-L2740 is the specification requirements for the X-07 lock and FF-L2740A. Below are the national stock numbers:

5340-01-357-6446 = X-07 Container Lock

5340-01-393-7058 = X-07 Door Lock

5340-01-381-6402 = CD X-07 Door Lock with drill resistant plate

5340-01-49-5776 = X-08 Container Lock

5340-01-469-5897 = CD-X08 Combination Deadbolt lock for pedestrian doors with drill resistant plate

5340-01-469-5906 = CD-X08 Combination Deadbolt lock for pedestrian doors with a non-drill resistance plate

5.20.5. (Added) Prior to storing classified information in a vault or secure room, the servicing civil engineer (CE) and the ISPM will survey the facility to determine if it meets the construction requirements outlined in DoD 5200.1-R, Appendix G and all other requirements of DoD 5200.1-R and AFI 31-401 for the storage of classified information. If the survey certifies that the facility meets requirements, the installation commander may approve the facility for storage of classified information. If the facility does not meet requirements, consider alternate or compensatory security controls in accordance with AFI 31-401, paragraph 5.30.1. Re-evaluate all secure storage rooms every 5 years and accomplish new approval letter and/or waiver requests.

5.21.1. Approve an area using key-operated locks to store bulky secret and confidential material according to paragraph **5.20.5. (Added)**.

5.21.2. As a minimum, lock and key custodians must be cleared to the level of the information stored in the area.

5.21.3. (Added) Control and store all keys at the level of security required for the information contained in the area.

5.23.2. Personnel having the combination will be recorded on SF Form 700. An additional SF Form 700 may be necessary for containers with more than five users.

5.23.4. (Added) Security Container combinations shall be changed every 2 years in the absence of one of the conditions specified in DoD 5200.1-R, para 6-404b.

5.28.3. Establish an annual clean-out day and include in your unit operating instruction.

5.29.1.1. (Added) For a listing of National Security Agency (NSA) evaluated and approved destruction devices see Annex B to NTISSI No.4004.

5.29.1.2. (Added) Post visual aids at shredders approved and not approved for destruction of classified. Note: Cross cut for shredders approved for destruction of classified must be a minimum of 1/32 x 1/2. AFRCVA 31-402, **AUTHORIZED FOR DESTRUCTION OF CLASSIFIED INFORMATION**, and

AFRCVA 31-403, **NOT AUTHORIZED FOR DESTRUCTION OF CLASSIFIED INFORMATION**, should be used and may be obtained from the AFRC Publications web site.

5.29.2.2. Safes required to have accountability control must ensure classified destroyed is annotated on accountability records.

5.30.1. HQ AFRC/SFI may approve or disapprove waivers.

6.3.2. Incorporate into the internal operating instruction to ensure only properly cleared individuals sign for incoming FedEx (or whoever holds current GSA contract), registered mail, first class mail with caveat "Return Service Requested", and Postal Service Express mail shipments. An AF Form 12, **Accountable Container Receipt**, or AF Form 310, **Document Receipt and Destruction Certificate**, must be completed anytime the material is transferred to a recipient not shown on the material's distribution. In addition, when using FedEx, registered mail, first class mail with caveat "Postmaster Do Not Forward," and Postal Service Express mail to send outgoing mail, personnel must verbally indicate whether the mail piece contains classified material to allow the Base Information Transfer Center (BITC) to verify delivery. (Reference, AFI 24-201, 7.8.1)

6.7.1.1. See sample Courier Letter at **Attachment 15 (Added)** and exemption notice at **Attachment 16 (Added)**.

6.8. Use DD Form 2501, **Courier Authorization**, whenever a person hand-carries classified information through an installation entry/exit point (expiration date is one year). The DD Form 2501 must be in their possession. The ISPM issues and maintains the DD Form 2501's. ISPMs may delegate to security managers.

8.3.4.1. Ensure the training requirements outlined in this chapter and in Attachment 7 are included in the organization's training plan in accordance with AFPD 36-22, **Military Training**, AFI 36-2201, **Developing, Managing, and Conducting Training**, AFMAN 36-2245, **Managing Career Field Education and Training**, and AFPAM 36-2211, **Guide for Management of Air Force Training Systems**. As a minimum, training documentation must include the trainee's name and grade, type of training (initial, refresher, or specialized), date of training, and a specific list of completed training subjects and tasks.

8.3.6. ISPMs ensure primary and alternate security managers are trained within 3 months of appointment. Security Managers receive documentation of training. Security Managers are responsible for providing information security program training to their units.

8.4. Cleared personnel are those personnel who have access to classified information (SAR code of 1, 2, 3, and S), are assigned to sensitive duties or are assigned to a critical sensitive position.

8.5. Uncleared personnel are those personnel who do not have access to classified information, and are not assigned to sensitive duties.

8.10.4.4. At all AFRC installations Security Forces, Intelligence, and the command post have the means of contacting their OSI agent and scheduling counterintelligence awareness briefings.

8.10.4.5. At all AFRC installations, prior to units being deployed, the Antiterrorism/Force Protection (AT/FP) representative coordinates with the appointed OSI agent. The AT/FP representative or Level II trained representative will administer the Level I Antiterrorism Awareness Training. OSI will supplement the Level I training by presenting a country specific briefing. The country specific briefing is classified Secret and will cover the current terrorism and criminal threat which exist at the deployed location. Level I training must be current within a six-month period prior to deployment.

8.11. Security managers ensure this training is accomplished.

8.14. If the person is terminating employment or separating from military service, the Authorized Requester will notify the Air Force Central Adjudication Facility (AFCAF) so that the refusal may be recorded in the DCII.

9.8.1. Appointment of inquiry official must be within 3 days after the incident was reported. The inquiry official will not be assigned to the same division/branch where the suspected incident took place. Provide the ISPM with a copy of the appointment letter.

9.8.1.2. Upon appointment, the inquiry official reports to the ISPM for a briefing.

9.8.2. The inquiry will also determine if the “subject(s) of the investigation” has completed all initial and recurring training requirements outlined in Chapter 8 and Attachment 7. Verification must include the date of initial training and all dates of recurring training.

9.11.2.1. Appointing official will close the investigation; however, the ISPM has the authority to elevate the decision should he/she disagree with the appointing official.

9.11.5. (Added) Retain a copy of the investigation. Maintain and dispose of records according to AFMAN 37-139, *Records Disposition Schedule*.

**Attachment 14 (Added)****SAMPLE SECURITY OPERATING INSTRUCTION**

**NOTE:** This attachment is provided to assist Unit Security Managers in developing an Internal Security Operating Instruction for their individual programs. This sample is not directive in nature. However it does include items which are, but only for demonstration purposes.

**Security****UNIT INFORMATION SECURITY PROGRAM****1. Appointment and Responsibilities:**

1.1. Commander/staff agency chief appoints the Unit Security Manager and establishes the training requirements. For example, the commander or staff agency chief appoints the Unit Security Manager. As a minimum, is trained by the local base Information Security Program Manager (ISPM).

1.2. Unit Security Manager responsibilities:

1.2.1. Provide advice and assistance to the commander or staff agency chief.

1.2.2. Schedule semiannual security self-inspections. The USM will not be assigned to conduct these inspections.

1.2.3. Attend meetings sponsored by the ISPM.

1.2.4. Maintain a current unit security program operating instruction.

1.2.5. Review and maintain a file of all semi-annual security self-inspection reports, Top Secret Control Account (TSCA) inventory reports, and security incident reports for a period of two years according to AFMAN 37-139, *Records Disposition Schedule*.

1.2.6. Provide security training for the unit.

1.2.7. Monitor security clearances to identify when additional investigative action is required.

1.2.8. Coordinate with respective supervisors and/or commander for the establishment of security information files (SIF). Also provide initial notification and subsequent status reports to base Security Forces concerning SIFs.

1.2.9. Monitor the implementation of the Personnel Security Program (PSP) requirements to include maintenance of the unit security clearance roster.

1.2.10. (Added) Review challenges to classification and assist personnel in complying with the classification markings and transmission procedures.

1.2.11. Ensure special access program authorizations are completed and maintained on file for assigned personnel. The most common special access programs affecting unit personnel are the North Atlantic Treaty Organization (NATO) and Critical Nuclear Weapon Design Information (CNWDI). Sensitive Compartmented Information (SCI) procedures are not addressed within this OI.

1.2.12. Maintain a USM handbook. Recommend the following be included: Security manager letter of appointment, internal security operating instructions, semiannual security self-inspection report, security manager meetings minutes, information letters, inspection checklists, program review report, annual training plan, and miscellaneous items deemed necessary for program management. This handbook should be a reference guide only and not contain any Privacy Act or other sensitive information, which may fall under the provisions of the rules For Official Use Only material

1.2.13. Notify personnel requiring a periodic reinvestigation (PR) of their security clearance and assist in completing required EPSQ and forms for submission.

1.2.14. Ensure the Personnel Security Program is evaluated during semiannual security self-inspections.

1.3. Top Secret Control Officer: (Use only if your organization handles or uses Top Secret.)

1.3.1. The commander or staff agency chief appoints the TSCO. The TSCO maintains a list of appointed alternate TSCOs.

1.3.2. Responsibilities: Monitors matters affecting accountability and control of Top Secret information and maintains the TSCA in accordance with current policy.

## **2. Authority to Classify or Declassify Information Classification Challenges:**

2.1. Original Classification Authority (OCA). The (insert the position title of your nearest OCA) is designated an OCA. In the OCA's absence, the person designated to act in his or her absence may exercise the classifier's authority. Only an OCA has the authority for subsequent extension in the duration of classification and regarding assigned levels of classification.

2.1.1. The authority to originally classify information is exercised sparingly and only when no other promulgated classification guidance exists for the information.

2.1.2. An action officer who develops information that is not currently classified and believes the information warrants safeguarding routes the information through channels to (OCA Office Symbol) for classification evaluation. Mark and safeguard the information in the same manner prescribed for the intended classification. The action officer is responsible for advising the USM of any OCA decision.

2.2. Derivative Classification Responsibility. Derivative application of classification markings is a responsibility of all assigned personnel who incorporate, paraphrase, restate, or generate in new form information that is already classified or those who apply markings according to OCA guidance.

2.3. Declassification Authority. (Insert OCA position title) has declassification authority over information they classify.

2.4. Classification Challenges. All personnel must challenge classification decisions that they believe are improper. Process the challenges through the unit Security Manager to the Information Security Program Manager.

**3. Marking Classified Material.** The originator of classified information is responsible for proper application of classification markings. The ultimate responsibility rests with the approver or signer of the document or material.

3.1. Those who prepare classified information are strongly encouraged to consult with their respective Security Manager and review DoD 5200.1R, Chapter 5, and DoD 5200.1PH, *A Guide to Marking Classified Documents*.

3.2. Refer complex marking issues to the Security Manager for assistance.

#### 4. Safekeeping and Storage:

4.1. Safe Custodians. The persons listed on the SF 700, **Security Container Information**, are considered safe custodians. A safe custodian:

4.1.1. Ensures safe combinations are changed as required.

4.1.2. Complies with the restrictions on the use of classified storage containers.

4.1.3. Ensures classified material over 5 years old is specifically designated for retention as required by records management procedures, according to AFI 37-138, ***Records Disposition- Procedures and Responsibilities***.

4.1.4. Reports containers that malfunction to the (enter organization responsible for making repairs), who will prepare appropriate paperwork to affect required repairs.

4.1.5. Ensures the contents of classified storage containers are identified in file plans. Personal "work files" of classified information are strongly discouraged but not prohibited. When necessary, these work files should be limited to specifically labeled folders and stored separately from the contents identified in the file plan.

4.2. Storing Top Secret Material. Store Top Secret information, to include Top Secret working papers, only at the Top Secret Control Account (TSCA).

4.3. Storing of NATO Material. Refer to unit OI or the NATO directives. (Use only if required.)

4.4. Storage of Any Other Classified Special Access Required Material. Consult the security authority for the Special Access Required (SAR) program on unique access and storage requirements. These SAR matters can vary from program to program.

4.5. Removal of Classified Material from the Unit:

4.5.1. Removal of classified information from the work place to take home to work on is not permitted.

4.5.2. Appropriately cleared personnel may remove classified information for the following purposes:

4.5.2.1. Routine destruction at the installation classified destruction facility.

4.5.2.2. Transporting classified material off of the installation as authorized by the Information Security Program Directive.

4.5.2.3. For approved hand carrying in travel status refer to the Information Security Program Directive.

4.6. End-of-Day Security Checks. Each (insert organizational element responsible) will establish a system to assure end-of-day (duty day) security checks are conducted within his or her area of responsibility to ensure that all unattended classified material is stored and locked in approved security containers. As a minimum, accomplish the following:

4.6.1. Ensure all classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers are placed in proper storage containers.

4.6.2. Check all desktops, file baskets, cabinet tops, trash containers, etc. for the presence of classified material.

4.6.3. Check all secure telephone units (STU) and any secure data fax machines for proper storage of crypto ignition keys (CIK) and ensure other secure telephone units are deactivated.

4.6.4. Check reproduction machines authorized for classified reproduction.

4.6.5. Ensure a person from each directorate is appointed, in writing, to conduct the end-of-day security check. This person rotates the combination dial of each container at least four times in the same direction and checks locking handle to assure the locked condition of the container. This person also enters the time of inspection and initials the "checked by" column of the SF 702, **Security Container Check Sheet**.

4.6.6. After checking SF 702 for all assigned security containers and performing inspections of each directorate office area, complete and sign the SF 701, **Activity Security Checklist**. Indicate the names of personnel working after the end-of-duty security check and, if applicable, their responsibility for securing a particular security container. If the designated person discovers unattended classified not properly stored or an unlocked security container during the check, he or she:

4.6.6.1. Assumes immediate custodial responsibility for the material or container.

4.6.6.2. Contacts the director or individuals listed on the SF 700. The contacted person responds and properly safeguards the unprotected classified material.

**5. Compromise of Classified Information.** Establish unit procedures for reporting compromise of classified information.

5.1. Reporting Information Security Incidents. Anyone who knows or believes that there may have been a compromise, loss, unauthorized disclosure, or other infraction affecting the safeguarding of classified information must report it without delay to the ISPM.

5.2. Appointing Investigation Officials. The commander/director who has responsibility for the area where the information security incident occurred appoints an investigator to conduct a investigation of information security incidents.

5.3. Briefing Requirements. The information security program manager briefs the person appointed to conduct the investigation. During these briefings the investigator is provided other technical guidance, such as consulting the local Staff Judge Advocate's office for legal guidance.

## **6. Access, Dissemination, and Accountability:**

6.1. Personnel Security Actions. Identify unit procedures to ensure members have the required personnel security investigation and clearance eligibility needed to perform officially assigned duties.

6.2. Dissemination Procedures. Establish procedures to ensure a person has the necessary clearance eligibility, and official "need-to-know," and SF 312 (Non-Disclosure Agreement) accomplished, prior to allowing access to classified information. Ensure unit members understand the responsibility rests with the person having custody of the material.

6.3. Reproduction Authority and Persons Designated to Copy Classified Material on Approved Copier:

6.3.1. Establish unit procedures for reproduction of classified material.

6.3.2. Include who (by position) approves the reproduction of classified information. Identify reproduction limitations, if any, for the material.

6.4. Top Secret Control Procedures (if applicable):

6.4.1. Identify constraints for working with such material.

6.4.2. (Office Symbol) manages the only TSCA for this (organization) and all Top Secret material, including working papers, will be stored in this account.

6.4.3. Not later than 31 January of each year, the TSCO re-controls the preceding year's Top Secret Register to the current year register.

6.4.4. Spell out procedures for conducting inventories of TS. For example, "The Commander appoints officials to conduct an inventory of the TSCA. The inventory is completed by the last duty day of February and the results are forwarded to the Commander not later than 15 March. Provide copies of both the appointment letter and inventory report to the Security Manager."

## **7. Transmission of Classified Material:**

7.1. General Explanation of Transmission Procedures Via Methods Other Than Electrical Messages:

7.1.1. Spell out procedures for Transmitting Top Secret material. For Example, "Transmit TS by an approved courier system or message or personal hand carrying by a designated representative. The US mail is never used to transmit Top Secret. Receipts are always used when transferring Top Secret material. AF Form 143 (for Top Secret only), AF Form 310, and AF Form 1565 are the most common receipt forms used for classified documents."

7.2. General Explanation of Local Unit Transmission Procedures:

7.2.1. (Insert office symbol of responsible official) is responsible for processing incoming receipts for classified documents. This responsibility includes:

7.2.1.1. Checking the contents of an accountable container against the enclosed receipt and promptly reporting any discrepancy. SC asks for assistance from the office of responsibility when classified parcels are large and bulky.

7.2.1.2. Returning receipts to senders of classified material.

7.2.2. Administrative personnel are responsible for:

7.2.2.1. Preparing receipts for material being transmitted.

7.2.2.2. Assuring "tracer action" requirements are followed.

7.2.2.3. Incoming classified material will not be placed in distribution boxes. Instead, material may be hand carried to the applicable action office or person, or they may be called for pickup by (responsible party's office symbol) personnel.

7.2.2.4. Incoming first class mail, registered, postal express, and Fed-Ex addressed to a person (excluding individuals) bearing the notice "Do Not Forward" will not be placed in distribution boxes. Secure all unopened mail, as described above, and first class mail in approved security containers at the end of each workday.

7.3. General Explanation of Hand carrying Classified on the Installation. Anytime classified information will be carried through an installation entry/exit point, unit personnel are required to be in possession of a DD Form 2501.

## **8. Disposal and Destruction:**

8.1. Annual "Clean Out" Day. A day during the first week of August will be devoted to the destruction of unneeded classified holdings.

8.2. Planning for Destruction. As soon as classified material has served its intended purpose, it should be processed for destruction. Destruction should be accomplished on a monthly basis to preclude the accumulation of unneeded material.

8.3. Retaining Classified Material Over 10 Years Old. Classified documents that are not permanently valuable records of the government shall not be retained more than 10 years from the date of origin, unless such retention is authorized by and in accordance with record disposition schedules.

8.4. Destruction Facilities:

8.4.1. The (insert organization responsible for base destruction facility) controls the base classified document destruction facility for paper products only. Call (insert phone and building number) for scheduling and other information.

8.4.2. Approved paper shredders may be used by unit personnel. They are located (insert locations of available shredders).

8.4.3. The (insert organization responsible for base destruction facility) controls the base classified destruction facility for film products and computer disks only. Call (insert phone and building number) for scheduling and other information.

8.5. Shipping Classified Records. Unless retirement is absolutely necessary, classified material will be destroyed according to AFMAN 37-139 *Records Disposition Schedule*. For packaging classified records, see AFI 37-138, *Records Disposition--Procedures And Responsibilities*, Chapter 6, on guidance when preparing documents and SF 135, Records Transmittal and Receipt, for shipment of classified records.

**9. Emergency Planning.** Procedures for the protection, removal, or destruction of classified material must be adhered to in the event of:

**9.1. Fire.** Return all classified material to the security container, if possible, and lock the container. If the material cannot be returned to the security container, the person possessing the material will maintain custody until relieved or the material is secured in an approved security container. If the classified cannot be removed from the building or the security container cannot be locked, the Fire Chief will be notified immediately. When the Fire Chief declares the area safe, all classified material or it's remains will be secured and the ISPM notified immediately.

**9.2. Tornado Or Natural Disaster.** Upon receiving warning of a tornado or severe weather, all classified material, which is not absolutely mission essential, should be placed in the security container and the container locked. If the classified material or security container is destroyed, scattered, or spirited away by natural forces, every effort will be made to find and secure the material or it's remains and contact the ISPM for additional guidance. Should a container be found following a severe storm, which damages the base and buildings housing containers, contact the ISPM, who maintains a listing of containers.

**9.3. Civil Disturbance.** All agencies will normally be warned in advance; however, should a disturbance occur without warning, return all classified material to the security container immediately and lock the container. The unit commander or staff agency chief determines if any additional protection is needed.

**9.4. Evacuation.** The installation commander may direct that all classified material be evacuated from (insert your installation). Regardless of the method used, personnel will ensure that all classified material is bagged, boxed, or crated and sealed as appropriate according to DOD 5200.1-R. An AF 310 will be accomplished indicating the number of containers, and the highest level of classified contained inside and the identity of the sending unit. An Evacuation Officer will be appointed by (insert your unit commander/staff agency chief) and will sign for each container.

**10. Semiannual Security Inspections.** Conduct semiannual security self-inspections, one between 1 January and 30 June and one between 1 July and 31 December. Security managers oversee the self-inspection but do not conduct it.

JOHN E. DOE, Colonel, USAF  
Commander

**Attachment 15 (Added)****SAMPLE COURIER LETTER**

(USE LETTERHEAD STATIONERY)

*Date*

MEMORANDUM FOR WHOM IT MAY CONCERN

FROM: *Office Symbol*

SUBJECT: Designation of Official Courier

1. Mr. John Doe, 022-22-2222, *office symbol, installation address*, is designated an official courier for the United States Air Force. Upon request, he will present his official identification card, number B0333444 and/or his DD Form 2501, Courier Authorization Form.

2. Mr. Doe is hand carrying two sealed packages, 8" x 8" x 24", addressed from *office symbol, installation address*, and addressed to *office symbol, installation address*. Each package is identified on the outside of the package by the marking "OFFICIAL BUSINESS. MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.

3. Mr. Doe is departing *Airport name* with a final destination to *Airport name*. He has a transfer point at *Airport name*.

4. This courier designation can be confirmed by contacting the undersigned at *office symbol, commercial number and DSN number*. This letter expires on *Date (not to exceed 7 days from date of issue)*.

JOHN G. SMITH, Col, USAF  
Commander

**Attachment 16 (Added)**

**SAMPLE EXEMPTION NOTICE**

**Department of the Air Force**

**Organization/Office Symbol**

**Installation**

-----  
**OFFICIAL BUSINESS**  
-----

**MATERIAL EXEMPT FROM EXAMINATION**

**Attachment 17 (Added)**

**PREPARING TOP SECRET REGISTER PAGES AND TRANSACTIONS**

**A17.1. (Added)** An AF Form 143, **Top Secret Register Page**, is generated by each office originating or receiving Top Secret information to establish formal accountability. If discrepancies are found, they must be resolved and/or annotated on the receipt prior to signing it and returning it to the sender. This action closes the sender's audit trail for that document.

**A17.2. (Added)** The new audit trail is initiated by completing two actions. Accountability is established by creating an AF Form 143 and an AF Form 144, **Top Secret Access Record and Cover Sheet**. Register pages are consecutively numbered and filed making up a Top Secret Register.

**A17.3. (Added)** The register is maintained by calendar year and may include active and inactive sections. In these cases the active section contains register pages for documents still on file. The inactive section contains register pages for documents that have been transferred, destroyed, downgraded, or declassified. Forms within these sections are filed based on the assigned register page number. The last page of each register is marked "THIS PAGE (99-SF-10) IS THE LAST PAGE OF THE TOP SECRET REGISTER FOR CALENDAR YEAR 1999." Inactive registers are retained for 5 years.

A17.3.1. (Added) To complete Part I (**Figure A17.1. (Added)**), the "Description of Document," transcribe the information exactly as it appears on the front cover of the document. Make sure it includes the OPR, type of document, date of document, the unclassified title, originator control number, copy number, and date the document was received. A file designation may be entered at the bottom of the block in pencil. The originator control number consists of the calendar year, office symbol, and consecutive number of Top Secret documents or material produced by the originator during the calendar year, e.g., 99-SF-1, 99-SF-2 and so on.

**Figure A17.1. (Added) Example of Part I. Description of Document.**

TOP SECRET REGISTER PAGE <i>(DO NOT enter classified information on this form)</i>							
I. DESCRIPTION OF DOCUMENT							
1. INDICATE ORIGINATOR, TYPE ( <i>letter, message, plan, etc.</i> ) DATE, UNCLASSIFIED SUBJECT TITLE, ORIGINATOR CONTROL NUMBER, AND COPY NUMBER(S). ALSO USE THESE DATA ELEMENTS FOR DESCRIBING ANY ATTACHMENTS THAT WOULD REQUIRE A RECEIPT IF TRANSMITTED SEPARATELY.							
1. INDICATE ORIGINATOR, ( <i>letter, message, plan, etc.</i> ) DATE, UNCLASSIFIED SUBJECT TITLE, ORIGINATOR CONTROL NUMBER, AND NUMBER(S). ALSO USE THESE DATA ELEMENTS FOR DESCRIBING ANY ATTACHMENTS THAT WOULD REQUIRE A RECEIPT IF TRANSMITTED.							
101 Wing Plan, 1 Jan 02, "HANDLING TOP SECRET MATERIAL," OCN: 02-12-11, Copy 13							
RECEIVED: 9 Jan 02							
FILED SF-01(file # in pencil)							
II. RECORD OF DOCUMENT CHANGES							
2. CHANGE NO.	3. COPY NO.	4. DATE	5. CLASSIFICATION	6. ORIGINATOR	7. ORIGINATOR CONTROL NO.	8. COPY NO. OF BASIC DOCUMENT POSTED TO	
III. DISPOSITION OF DOCUMENT							
SECTION 1							

A17.3.2. (Added) Part II (**Figure A17.2. (Added)**), the "Record of Document Changes," is used to establish active accountability of Top Secret changes to the basic document. In addition to entering the change number in item 2, also enter the date the change was received. The remainder of the items is self-explanatory. Enter all changes (Classified and Unclassified) to show the complete status of the basic document. Use the alphabetical letters A, B, C and so on to prepare continuation pages to the basic form.

**Figure A17.2. (Added) Example of Part II. Record of Document Changes.**

II. RECORD OF DOCUMENT CHANGES							
2. CHANGE NO.	3. COPY NO.	4. DATE	5. CLASSIFICATION	6. ORIGINATOR	7. ORIGINATOR CONTROL NO.	8. COPY NO. OF BASIC DOCUMENT POSTED TO	
1- RCVD 17 Jan 02	13	20020114	TOP SECRET	101 Wing	02-12-11		
III. DISPOSITION OF DOCUMENT							
SECTION 1							
9. COPY NO.	10. TO	11. DATE	12. TYPE OF ACTION	13. SIGNATURE			

A17.3.3. (Added) Part III (**Figure A17.3. (Added)**), the "Disposition of Document" section, is used to show the disposition for each document; however, if the disposition of multiple copies is the same, all copy numbers can be included in item 9, i.e., Copies 1, 2, 3, or 1 through 3. Items 10a through 13a are used when accountability is transferred to an official of another TSCA on the same installation. If the material is sent off the installation, enter "SEE ATTACHED RECEIPT" in item 13a. A copy of the AF Form 310 or AF Form 1565 is held in suspense until a signed receipt is returned from the receiving TSCA. The signed receipt is attached to the applicable register page.

**Figure A17.3. (Added) Part III. Disposition of Document.**

III. DISPOSITION OF DOCUMENT				
SECTION 1				
9. COPY NO.	10. TO	11. DATE	12. TYPE OF ACTION	13. SIGNATURE
	A. HQ ACC/SF	A. 20020129	A. ACCOUNTABILITY TRANSFERRED	A. George OJungle
	B.	B.	B. ACTION, REVIEW, OR COORDINATION	B.
		C. 20020131	C. DOCUMENT RETURNED	C. Harley Davidson
		D.	D. DOCUMENT DESTROYED	D.
		E.	E. COMMITTED TO CENTRAL DESTRUCTION FACILITY	E.
		F.	F. OTHER (Specify)	F.
		G.	G. AUDITED	G.
SECTION 2				
9. COPY NO.	A.	A.	A. ACCOUNTABILITY TRANSFERRED	A.

A17.3.4. (Added) Part III continued (Figure A17.4. (Added)), Items 10b, 11b, and 13b are completed when a TSCO temporarily transfers a Top Secret document to another TSCO for review, coordination or action. These items are not completed when the document is temporarily given to an individual serviced by the TSCO. The AF Form 614, Charge Out Record, is used in this case to show who has the document and its location. Items 11c and 13c are completed when a document is returned to the original TSCO following action, review or coordination. Items 11d and 13d are completed when the document is to be destroyed. Two appropriately cleared persons must complete the destruction process.

Figure A17.4. (Added) Part III, items 10b, 11b and 13b.

SECTION 2				
9. COPY NO.	A.	A.	A. ACCOUNTABILITY TRANSFERRED	A.
	B. HQ ACC/SFI	B. 20011218	B. ACTION, REVIEW, OR COORDINATION	B. Dudley Doright
		C. 20011218	C. DOCUMENT RETURNED	C. Harley Davidson
		D. 20011218	D. DOCUMENT DESTROYED	D. Fred Flintstone
		E.	E. COMMITTED TO CENTRAL DESTRUCTION FACILITY	E.
		F.	F. OTHER (Specify)	F.
		G.	G. AUDITED	G.
14. REGISTER PAGE NO. 01-DO-13			15. RECONTROLLED FROM REGISTER PAGE NO.	16. RECONTROLLED TO REGISTER PAGE NO. 02-DO-10

AF FORM 143, 19820901 (EF-V2) PREVIOUS EDITION WILL BE USED.

A17.3.5. (Added) Part III continued (Figure A17.5. (Added)) Items 11e, 13d and 13e are completed when the document is committed to a Central Destruction Facility (CDF). Two signatures of appropriately cleared unit personnel will sign Item 13e. As necessary, enter the date and serial number assigned to the bag containing Top Secret documents.

Figure A17.5. (Added) Part III, Items 11e, 13d and 13e.

SECTION 2				
9. COPY NO.	A.	A.	A. ACCOUNTABILITY TRANSFERRED	A.
	B. HQ ACC/SFI	B.	B. ACTION, REVIEW, OR COORDINATION	B.
		C.	C. DOCUMENT RETURNED	C.
		D.	D. DOCUMENT DESTROYED	D.
		E. 20011220	E. COMMITTED TO CENTRAL DESTRUCTION FACILITY	E. Fred Flintstone
		F.	F. OTHER (Specify)	F.
		G.	G. AUDITED	G.
14. REGISTER PAGE NO. 01-DO-13			15. RECONTROLLED FROM REGISTER PAGE NO.	16. RECONTROLLED TO REGISTER PAGE NO. 02-DO-10

AF FORM 143, 19820901 (EF-V2) PREVIOUS EDITION WILL BE USED.

A17.3.6. (Added) Part III continued (**Figure A17.6. (Added)**), Items 11f, 12f, and 13f are used to specify other transactions affecting the document or register pages, such as, the date and authority of any downgrading or declassification action.

**Figure A17.6. (Added) Part III, items 11f, 12f and 13f.**

9. COPY NO.	A.	A.	A. ACCOUNTABILITY TRANSFERRED	A.
	B. HQ ACC/SFI	B.	B. ACTION, REVIEW, OR COORDINATION	B.
		C.	C. DOCUMENT RETURNED	C.
		D.	D. DOCUMENT DESTROYED	D.
		E.	E. COMMITTED TO CENTRAL DESTRUCTION FACILITY	E.
		F. 20011220	F. OTHER (Specify) DECLASSIFIED	F. Harley Davidson
		G.	G. AUDITED	G.
14. REGISTER PAGE NO. 01-DO-13			15. RECONTROLLED FROM REGISTER PAGE NO.	16. RECONTROLLED TO REGISTER PAGE NO. 02-DO-10

AF FORM 143, 19820901 (EF-V2) PREVIOUS EDITION WILL BE USED.

A17.3.7. (Added) Part III continued (**Figure A17.7. (Added)**), Items 11g and 13g are completed for each inactive section of all register pages during Top Secret inventories. The signature of the Top Secret inventory official in 13g reflects the official's concurrence regarding proper disposition of documents.

**Figure A17.7. (Added) Part III, items 11g and 13g.**

SECTION 2				
9. COPY NO.	A.	A.	A. ACCOUNTABILITY TRANSFERRED	A.
	B. HQ ACC/SFI	B.	B. ACTION, REVIEW, OR COORDINATION	B.
		C.	C. DOCUMENT RETURNED	C.
		D. 20011220	D. DOCUMENT DESTROYED	D. Harley Davidson
		E.	E. COMMITTED TO CENTRAL DESTRUCTION FACILITY	E.
		F.	F. OTHER (Specify)	F.
		G. 20020102	G. AUDITED	G. Adam West
14. REGISTER PAGE NO. 01-DO-13			15. RECONTROLLED FROM REGISTER PAGE NO.	16. RECONTROLLED TO REGISTER PAGE NO.

AF FORM 143, 19820901 (EF-V2) PREVIOUS EDITION WILL BE USED.

A17.3.8. (Added) Part III, Item 14 identifies the register page number. The TSCO assigns a consecutive number by including the calendar year and TSCA functional address symbol, e.g., 99-XP-04. This number provides a system to assist in the documentation of an audit trail. If additional space is needed to establish accountability of a document, create an additional AF Form 143 and add the alphabetical letter A, B, C, to the original register page number, e.g., 99-XP-04A.

A17.3.9. (Added) Part III, Item 15 reflects the register page number of the previous calendar year's register. This number assists when following the audit trail back to the receipt or generation of a Top Secret document.

A17.3.10. (Added) Part III Item 16 (**Figure A17.8. (Added)**), reflects the new register page to which the documents are being re-controlled when re-controlling an entire page. This number helps to follow the audit trail forward to locate the document or its disposition.

**Figure A17.8. (Added) Part III, item 16.**

	F.	F. OTHER (Specify)	F.
	G.	G. AUDITED	G.
14. REGISTER PAGE NO. 01-DO-13	15. RECONTROLLED FROM REGISTER PAGE NO. 99-DO-15		16. RECONTROLLED TO REGISTER PAGE NO. 02-DO-10

AF FORM 143, 19820901 (EF-V2) PREVIOUS EDITION WILL BE USED.

**A17.4. (Added)** Access to specific Top Secret information is documented using the AF Form 144. This form is attached to each Top Secret document to identify all persons given access to the information and the date of disclosure. The person accountable for the information assures the recording is accomplished prior to disclosure. A person's name must appear only once; regardless of the number of times the individual is subsequently given access. Additional required information is self-explanatory. The remarks section is used to reflect:

A17.4.1. (Added) The unclassified title.

A17.4.2. (Added) Special Access Program identifiers (e.g., SIOP Category 4, CNWDI, NATO, etc.).

A17.4.3. (Added) Warning notices (e.g., WNINTEL, NOFORN, etc.).

A17.4.4. (Added) Appropriate copy number.

**A17.5. (Added)** The AF Form 144 is kept with each document at all times and removed only when the document is destroyed, downgraded, or declassified. The forms are then filed by calendar year and register page number and maintained for two years.

**A17.6. (Added) Reproduction:**

A17.6.1. (Added) Originators of Top Secret material must keep account of the number of copies made and a list of the recipients. For example, enter "Copy 1 of 20 Copies" on the document and show the recipient on the file or record copy. If a subsequent printing of 10 additional copies becomes necessary, the next number would begin with "Copy R21 of R30 Copies," and so on.

A17.6.2. (Added) Copies that are made by an office other than the originator, with the approval of the originator, are identified by an "RC" (reproduced copy) before the copy number. For example, if 5 copies were reproduced, then Section I of the AF Form 143 would show a notation such as, "Reproduced 5 copies on (date) by authority of (authorizing agency), "RC1 of 5RC, RC2 of 5RC, and so on. For messages, the recipient enters their own copy number for accountability purposes, e.g., "Copy 1 of 2 Copies", etc.

A17.6.3. (Added) An office other than the originator shows the following on reproduced material:

A17.6.3.1. (Added) Reproduced on (date) by authority (identify authorizing agency).

A17.6.3.2. (Added) Reproduced copy\_\_ of\_\_ reproduced copies.

A17.6.4. (Added) The office of origin is listed as the authorizing agency when reproduction is authorized in the document.

A17.6.5. (Added) A telecommunications center or distribution activity may reproduce, without approval of the originator, a sufficient number of copies needed to meet initial distribution requirements shown in the address element. A reproduction entry is not used in these instances. Any additional reproduction of Top Secret messages, which do not include reproduction authority, requires approval from the originator. Again, all reproduced Top Secret material must be entered in the Top Secret Register.

**A17.7. (Added) Receipts:** Top Secret information must be transmitted using a continuous chain of receipts. Three types of receipts can be used in the audit trail for a Top Secret document.

A17.7.1. (Added) AF Form 143, Top Secret Register Page:

A17.7.1.1. (Added) This form is used as a receipt when transferring Top Secret material from one TSCO to another on the same installation. This includes material being released to the Telecommunications Center (TCC). The customer service representative at the TCC completes items 10b, 11b, and 13b prior to transfer.

A17.7.1.2. (Added) When transmission or processing is complete, the service representative returns all original material to the user or requesting agency. The controlling TSCO completes items 11c, and 13c to reflect the return of the Top Secret material to the TSCA.

A17.7.2. (Added) AF Form 1565, Entry, Receipt, and Destruction Certificate:

A17.7.2.1. (Added) This form is a multipurpose form and can be used as a receipt when transmitting changes to a Top Secret plan or similar document. The sender annotates the AF Form 143 controlling the change by completing item 11a, which shows the agency of the intended recipient and item 13a, which states "See Attached Receipt." A copy of the receipt is kept in suspense pending return of the signed receipt or for use as a tracer, if necessary. The sender also transmits sufficient copies for each basic document held by the recipient to provide the following:

A17.7.2.2. (Added) One copy to be used as a receipt.

A17.7.2.3. (Added) One copy to post or certify entry of changed pages to the basic document.

A17.7.2.4. (Added) One copy to certify destruction of pages removed from the basic document.

A17.7.2.5. (Added) AF Forms 1565 returned as receipts are attached to the register page by the sending TSCO. As active documents are re-controlled to the next year's register, the AF Form 1565 used as receipts/destruction certificates are retained with the old register pages. This procedure helps to clean up and reduce the size of the current register.

**A.17.8. (Added) Top Secret Inventory Procedures:**

A17.8.1. (Added) Top Secret inventories are conducted upon change of the TSCO or at intervals not to exceed 12 months.

A17.8.2. (Added) The inventory includes two major components; sighting of all active documents and an audit of all inactive sections of the register, and a review of all Top Secret control procedures for compliance.

A17.8.3. (Added) The TSCO appointing authority appoints, by letter, a person with the proper clearance, access and knowledge of Top Secret control procedures to conduct the inventory. TSCOs and alternates

may not participate as inventory officials or team members. (Exception: A succeeding primary TSCO may conduct an inventory upon initial appointment.)

**A17.9. (Added) Sighting Procedures:** The sighting portion of the inventory physically locates each document for which a register page reflects the TSCO is accountable. This includes documents that are on loan to another TSCA or stored at a location geographically separated from the TSCA. The sighting portion also assures that all Top Secret documents on file have been entered into the register.

**A17.10. (Added) Audit Procedures:**

A17.10.1. (Added) The audit portion of the inventory determines that all pages of the register are on file. Inactive sections showing final disposition of documents are audited, for example:

A17.10.1.1. (Added) A receipt covering transfer of the document.

A17.10.1.2. (Added) A re-control statement to another register page.

A17.10.1.3. (Added) Authority to downgrade or declassify the document.

A17.10.1.4. (Added) Certificate of destruction.

A17.10.2. (Added) The inventory official should review registers to ensure that the previous inventory official did not overlook inactive sections. If an entry is improper or unclear, the inventory official determines its meaning and records the findings in the inventory report. A register page section is audited when the inventory official dates item 11g and signs item 13g. Inactive sections are audited only once. Sections reflecting a document is on temporary loan or a suspense receipt is being held are not audited. Active register pages are not audited.

**A17.11. (Added) Inventory Report:**

A17.11.1. (Added) The inventory official must also inquire into compliance with all Top Secret control procedures and record the findings in the inventory report.

A17.11.2. (Added) The inventory report must include the names and full signatures of the inventory officials and be in sufficient depth to explain compliance or non-compliance with all Top Secret control procedures.

**A17.12. (Added) Report Endorsement:** The TSCO appointing authority endorses the report outlining corrective actions that must be taken. The appointing authority must also certify that all Top Secret material within the TSCA is needed for mission accomplishment. A copy of the report with the appointing authority's endorsement, and corrective actions taken, must be maintained for review during the next inventory. A sample inventory report is shown in Figure 5-1.

**A17.13. (Added) Closing A TSCA:** To close (or disestablish) a TSCA, destroy or transfer all Top Secret material, completing the appropriate disposition portions of all active register page sections. The TSCA appointing authority appoints a Top Secret inventory official to complete a final inventory and formally disestablishes the TSCA in the endorsement approving the inventory. All inactive files must be maintained in accordance with AFI 37-139, Volume II (five years).

JAMES E. SHERRARD III, Lt General, USAF  
Commander