

7 October 2002



Security

4TH AIR SUPPORT OPERATIONS GROUP SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the 4th Air Support Operations Group website at: <http://www.usafe.4asog.af.mil>. If you lack access, contact the 4 ASOG Commanders Support Staff.

OPR: 4 ASOG/Security Manager

Certified by: 4 ASOG/CD

Distribution: F

Pages: 22

PURPOSE: This Operating Instruction establishes policies and procedures governing the security program within the 4th Air Operations Support Group. It applies to all military, civilian, and contractor personnel assigned to the 4 ASOG. It defines individual roles in program management and assigns specific responsibilities to functional managers. The program is designed to provide increased security awareness and education to all personnel responsible for safeguarding Air Force operations and sensitive national defense information at all times and under all circumstances. It implements DoD 5200.1-R, Information Security Program; AFI 31-401, Managing the Information Security Program; AFI 31-406, Applying North Atlantic Treaty Organization (NATO) Protection Standards; AFI 31-501, Personnel Security Program Management; AFI 31-601, Industrial Security Program Management; and AFI 16-701, Special Access Program. Reference to the word “unit” in this instruction refers to squadrons and detachments and or their personnel assigned to.

1. Responsibilities.

1.1 Each group, squadron, and detachment commander will appoint in writing a primary and alternate unit security managers (USM), to ensure compliance with security directives for the protection of classified material for 4 ASOG. The original memorandum of appointment will be sent to the Security Forces Information Security staff (86 SFS/SFAI). This memorandum will help them identify a single point of contact within the directorate for security matters.

1.1.1. Ensure primary and alternate unit security managers receive training for their assigned security programs and duties within 90 days of appointment (IAW AFI 31-401).

1.1.2. Delegate, via appointment letter, NATO access granting authority to the unit security managers.

1.1.3. Designate in writing equipment and personnel approved for classified reproduction

1.1.4. Follow security incident provision in paragraph 2.8 when appropriate.

1.2. Group Security Manager Responsibilities. Review and update this operating instruction annually and ensure compliance.

1.3. Unit Security Manager Duties for Information Security, Personnel Security and Industrial Security Programs.

1.3.1. The unit security manager will personally implement and oversee all elements of an effective security program addressing information, personnel, industrial, resources security.

1.3.2. Provide advice and assistance to the commanders and unit personnel on security related issues and ensure compliance with security directives.

1.3.3. Ensure a copy of the group operating instruction for security guidance is implemented and followed, and electronic or hard copies of applicable instructions, as stated in introduction paragraph of this instruction, are accessible.

1.3.4. Ensure unit personnel receive initial and quarterly refresher training.

1.3.5. Monitor semi annual internal self-inspections IAW 86 SFS checklist.

1.3.6. Attend scheduled 86 SFS/SFAI security manager's meetings or ensure a unit representative attends.

1.3.7. Assist and provide guidance to those involved in security incidents (i.e., inquiry/investigating official and appointing authority). Monitor security incidents from initiation to closing, ensuring timely reporting of the incident and submission of reports.

1.3.8. Develop local Emergency Protection Plan with unit commander signature and post in area.

1.3.9. Ensure each Commanders Support Staff / Mail handlers are aware of provision of paragraph 2.2.6 of this instruction.

1.3.10. Assist unit personnel in updating security clearances. Upon notification, unit personnel have 30 days to complete the process. The Electronic Personnel Security Questionnaire (EPSQ) is a personal computer-based program used to simplify the process of reporting the information required to obtain and update as needed a security clearance. A copy of the software is provided to individuals needing a clearance update. Initiate AF Form 2583 (Request for Personnel Security Action) to document a local files check, which is a

review of locally available medical, personnel and security police records to determine if there is any unfavorable information. For top secret access, DD Form 1879 is required.

1.3.11. Coordinate on all change requests to the Unit Manning Document (UMD) relating to Security Access Requirement (SAR CODE).

1.3.12. Brief personnel and maintain AF Form 2583 in the security manager's files on each individual requiring NATO access. Individuals must be debriefed by the unit security manager by completing the AF Form 2587, when access is no longer needed (i.e., PCS/PCA/TDY 90 days or more).

1.3.13. Complete AF Form 2587 (Security Termination Statement) for every military or civilian member retiring or separating from the service. Additionally, civilian employees with special access terminating employment for more than 60 days need to complete AF Form 2587. The unit security manager will maintain AF Form 2587 in inactive files for 2 years.

1.3.14. Issue Courier Authorization Letters.

1.3.15. Maintain documentation identified in Section G of 86 SFS self inspection checklist.

1.3.16. Ensures that this program governs the protection of classified defense information in the hands of government contractors doing business with the government.

1.3.17. Request and receive visit authorization letters for all industrial contractors working within the unit and provide clearance verifications.

1.3.18. Maintain liaison with all contractors, field representatives and the base industrial security personnel providing security support as required.

1.3.19. Maintain a security manager's handbook. (See USAFE Sup 1, to AFI 31-401)

1.4. Duties of the unit security manager as the SCI billet manager. This is handled for the 4 ASOG by the Third Air Force Security Office.

1.5 Reporting investigator responsibilities.

1.5.1. Attends training, writes investigation report IAW 2.8, brief CC; forward report to 86 SFS.

2. Procedures.

2.1. **Storage, handling, and transmission of classified material.** Classified materials will be received, handled, stored, and transmitted IAW DoD 5200.1-R and AFI 31-401. The unit commander may approve "in writing" open storage of classified for vaults and for secure rooms. Contact the unit security manager for approval instructions.

2.1.1. Security Storage Containers: Safes/Vaults/SCIFs

2.1.1.1. Incoming classified material will be stored in a container having a built-in, three-position, dial-type combination lock approved by GSA or a Class A/B vault or vault type room that meets the standards established by the head of the DoD Component concerned (USAF).

2.1.1.2. Every security container must have a primary and alternate safe custodian appointed in writing and forwarded to the unit security manager.

2.1.1.3. All security containers must be assigned an identification number.

2.1.1.4. Security containers/vault custodians must accomplish inspections of the container IAW TO 00-20F2, Inspection and Preventive Maintenance Procedures for Classified Storage Containers, to ensure it is authorized for storage of classified. Document inspection on the AFTO Form 36, Maintenance Record for Security Type Equipment.

2.1.1.5. AF Form 793 (In case of Emergency) and AF Form 1356 (Warning Facility Protected by an Intrusion Detection System) or locally developed equivalent; will be posted on vault or SCIF doors.

2.1.1.6. Personnel opening/closing the secure room will use the SF 702 (Security Container Check Sheet) and will check exterior before opening and interior after opening to determine evidence of forced entry or pilferage. If such evidence is found, the law enforcement desk sergeant and the unit security manager will be notified immediately. If COMSEC material is involved, the COMSEC custodian will be notified. If SCI material is involved, the local SSO will be notified.

2.1.1.7. Unescorted access to a secure room will be controlled and limited to personnel cleared for access. Additionally, personnel must have a need-to-know to perform official duties. Positive identification will be made for an individual requesting access. If the individual is not cleared, but has a valid reason for entry, the area will be sanitized and personnel within the area will be made aware of their presence. To sanitize the area before uncleared personnel enter, remove all classified material from immediate or open view and do not discuss classified information.

2.1.1.8. Each individual authorized access to any secure room is responsible for knowing and understanding procedures for accessing and securing these areas. Once opened, the vault or secure room must be manned at all times or be secured.

2.1.1.9. Combinations to containers/vaults/secure rooms will be given only to those personnel requiring access on a regular basis. Custodians will notify authorized personnel of changes. The stored combination will be kept in a sealed SF 700 and marked with the appropriate office

symbol, safe number, and stamped with the highest classification stored within the container/secure room. The envelope should include a list of individuals who are authorized the combination. IAW AFI 31-401, paragraph 5.23.3 “When SF Form 700, Part II is used to record a safe combination, it must be, marked with the highest classification level of material stored in the security container and stored in a security container other than the one for which it is being used.” If you do not use part II to write down the combination, there is no need to mark or store it.

2.1.1.10 Combinations to containers/vaults/secure rooms will be changed when approved personnel PCS, PCA, separate, retire, a compromise has occurred, or when an individual no longer require access, when maintenance is performed, or at least annually.

2.1.1.11. Non-SCI facilities with safes are not required to record the combinations on an SF 700, Part 2A; however, if you decide to store the combination, Part 2A should be sealed in an envelope, labeled with the appropriate office symbol, safe number, and stamped with the highest classification stored in the safe and stored in another safe. Additionally, a list of personnel who are authorized access to the safe should be included. Safe custodians will detach SF 700, Part 1, attach it to the inside of safe, and ensure only personnel requiring regular access are given the combination and notified of any changes.

2.1.1.12. Resource Modification/Relocation. When physical security properties of the secure room (i.e., floors, walls, ceilings, doors, etc.) are modified or when resources being protected are relocated, 86 SFS/SFAI must have prior notification, in writing.

2.2. Handling.

2.2.1. Individuals are authorized to review, handle, receive and process classified information equal only up to their clearance level.

2.2.2. All personnel who handle or process classified material are responsible for providing protection and accountability for the material at all times. Always keep classified material under your control and protect documents with cover sheets.

2.2.3. All computer products created on accredited systems will be classified as “system high” until reclassified or declassified by the Original Classification Authority (OCA). Products will be accounted for, controlled, marked and protected in accordance with the assigned classification. Working papers containing classified information shall be dated when created and annotated with the organization, office symbol, and phone number of the originator. Working papers will be destroyed when no longer needed.

2.2.4. Magnetic media will be marked, stored and handled IAW AFI 31-401, Chapter 4.

2.2.5. When loaning out classified material within or outside the organization, use an AF Form 614 (Charge Out Record) to establish a suspense for returning material.

2.2.6. All registered mail will be treated and protected as classified until the classification of the contents can be verified.

2.2.7. Marking “Derivatively Classified” Documents. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the markings of the source information. As with documents created by original classifiers, each derivative document must have portion markings and overall classification markings. Identify the source used as the basis for classification on the “Derived from” line of the derivative document. The “Declassify on” line of the source document is carried forward to the “Declassify on” line of the derivative document.

2.3. Reproducing classified material. Classified reproduction should be kept to the minimum required to accomplish the mission. All copies are subject to the same controls and safeguards as the original document. Contact unit security manager for additional guidance.

2.3.1. Portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Record the number of copies reproduced and the identity of each recipient on the original document. The OPR must be notified when copies are destroyed.

2.3.2. USAFE CSS/SCBPC approves equipment for classified reproduction.

2.3.3. Marking Equipment. The following statement should be posted when copier has been approved for classified reproduction: “THIS EQUIPMENT AUTHORIZED FOR REPRODUCTION OF CLASSIFIED MATERIAL”. The following statement should be posted when the copier has NOT been approved for classified reproduction: “STOP, DO NOT USE THIS MACHINE FOR CLASSIFIED REPRODUCTION”.

2.4. Hand-carrying Classified Material. Classified material may be removed from the unit only in the performance of official duties. The provisions of DoD 5200.1-R/AFI 31-401, Chapter 6, apply for transmitting/transporting classified information. Individuals authorized to hand-carry classified material shall be fully briefed of these provisions. Whenever classified information is transported outside the work area, it shall be enclosed in a sealed envelope, double wrapped, folder, or other closed container (locked briefcase) to prevent loss or observation. Furthermore, you must have official written authorizations signed by the commander: a Designation of Official Courier Memorandum, and an Exemption Notice (both the memorandum and the exemption notice must be in English and any other country language whom personnel will have opportunity to enter; i.e., Poland, France for TDY purposes). Additionally, consideration must be given to mode of transportation, time sensitivity, authorized storage availability at the destination, transfer or accountability at destination, or method of returning material. Contact the security office for instructions. Use the following guidance for hand-carrying classified material:

2.4.1. On Base, with no entry/exit inspection points. Verbal authorization from the unit commander is required for hand-carrying classified information between buildings or areas within the confines of the installation.

2.4.2. On base, with entry/exit inspection points. You must have a Courier Authorization Letter and Exemption Notice.

2.4.3. Outside your duty location area. When hand-carrying any classified information outside the confines of your duty location area or Germany, you must have an official courier memorandum, and an exemption notice. Also the letter will be in the language of the host nation you are located in and going to.

2.4.4. Commercial. Hand-carrying classified material on a commercial aircraft must be approved by the unit commander, providing all requirements are met IAW AFI 31-501, DOD 5200.1-R, paragraph 7-302(e). If travel involves passage through an inspection point where classified may be subject to examination by non-DoD personnel or involves overnight stopovers, contact the unit security manager for proper procedures.

2.5. Mailing.

2.5.1. SECRET. The only approved method of mailing SECRET material is US Registered Mail. Air Force Form 310, Document Receipt and Destruction Certificate, is required. Contact unit security manager for proper procedures.

2.5.2. Confidential. The only approved methods of mailing Confidential material are US Registered Mail and US Certified Mail. No receipt is required unless Special Access Program is involved. Contact unit security manager for proper procedures.

2.6. Foreign Travel Policy:

2.6.1. Each member is responsible for maintaining a list of their foreign travel. This information will be used when completing clearance updates.

2.6.2. Members who have access to SCI information must submit any anticipated leisure travel to foreign countries to the unit security manager, or report any travels within 3-days upon return. The security manager will ensure personnel receive proper briefings if threat conditions exist in the areas of travel. Individuals will report contacts of a suspicious nature to their supervisor, security manager or local OSI upon return.

2.7. Disposal of Classified

2.7.1. Classified material will be destroyed as soon as it has served its purpose and shall be destroyed by an approved crosscut shredder. Destruction of classified material and documentation of destruction will be accomplished as follows:

2.7.1.1. **TOP SECRET:** Two people with appropriate clearance must be present and a destruction certificate must be completed (AF Form 143, Top Secret Register Page, when using AF Form 1556, file it with AF Form 143) with two signatures.

2.7.1.2. **SECRET and CONFIDENTIAL:** IAW AFI 31-401, paragraph 5.29.2.2. A record of destruction is not required but an appropriately cleared person must be involved in the destruction process. No destruction certificate is required.

2.7.1.3. IAW AFI 31-406, paragraph 5.12.2. NATO Secret requires a destruction certificate with two signatures. AF Form 310 or 1556 can be used for the destruction certificate. File destruction certificate in IAW AFMAN 37-139.

2.7.2. Classified magnetic media will be properly protected and stored until degaussed. Destruction records are not required.

2.7.3. Emergency destruction or relocation of classified material will be done by personnel IAW Emergency Protection Plans for the vault, container or secure room which holds the classified material.

2.7.4. **Annual Clean-Out Day:** The second Wednesday of February is the USAFE clean-out day. IAW AFI 31-401/USAFE SUP, Chapter 9, this day is designated to purge and destroy all unneeded classified holdings. Normal documentation is required.

2.8. Security Incidents. A security incident may result in damage to our national security. Security incidents are normally caused by a violation of established procedures for handling, storing, transferring, or accounting of classified information. In the event of a violation and the material discovered is classified, secure it immediately and report the incident to the supervisor, security manager or commander.

2.8.1. **Conducting inquiries or investigations.** A preliminary inquiry is conducted whenever a security incident involving classified information occurs. The categories of security incidents are:

2.8.1.1 **COMPROMISE:** The disclosure of classified information to persons not authorized.

2.8.1.2. **POTENTIAL COMPROMISE:** When an investigating official concludes that a compromise probably occurred as a result of the security incident.

2.8.1.3. **SECURITY INFRACTION:** An incident that involves the misuse or improper handling of classified material, but does not fall into the categories of compromise, probable compromise, or inadvertent access.

2.8.2. Once the group/squadron or detachment commander gains knowledge of a security incident, he/she is responsible for initiating a preliminary inquiry under DoD 5200.1-R/AFI 31-401, chapter 9. The commander will ensure:

2.8.2.1. The incident is reported to 86 SFS/SFAI within one duty day.

2.8.2.2. A preliminary inquiry officer (IO) is appointed in writing. Security managers will not be appointed. A field grade officer, MSgt, or GS-09 or above will be appointed. Individuals appointed should be of a higher grade than the person suspected of causing the incident. The individual appointed should not be from the same office in which the incident occurred.

2.8.2.3. The report will be completed within 30 duty days from the date of appointment or request an extension in writing and must be submitted to the commander.

2.8.3. Duties of the preliminary inquiry officer.

2.8.3.1. The IO must contact 86 SFS/SFAI for a briefing for technical guidance in conducting the inquiry.

2.8.3.2. Consider the circumstances surrounding the incident and assign a category for the incident.

2.8.3.3. Question personnel involved. Identify person(s), acts, conditions which caused the incident.

2.8.3.4. Complete report and have the security manager review the report. The investigating officer then forwards the report to 86 SFS/SFAI.

2.8.4. Duties of the security manager for security incidents.

2.8.4.1. Assist and provide guidance to those involved in the security incident (i.e., inquiry/investigation official and appointing authority).

2.8.4.2. Be familiar with directives concerning security incidents.

2.8.4.3. Ensure security incidents are reported to the 86 SFS/SFAI within one duty day of discovery.

2.8.4.4. Monitor security incident from appointment to closing.

2.9. Security Awareness. A good security education program is the key to attaining a solid security program. It is imperative training be taken seriously and be accomplished in a manner that stresses the importance of security.

2.9.1. Each unit security manager will ensure all military, GS civilians, and contractors receive the required quarterly security awareness and motivation training IAW AFI 31-401, Chapter 7.

2.9.2. Supervisors will verify newcomer's security clearances through the unit security manager prior to allowing them to perform any function involving access to classified information. Supervisors will brief all incoming personnel on security requirements and practices within their work center. Supervisors will ensure all newcomers report to the unit security manager within 30 duty days of arrival for security in-processing.

2.10. Security Inspections. Security self-inspections will be conducted on a semi-annual basis. The self-inspection official will be appointed in writing by the commander. Security managers will not be appointed. Attachment 3 of this OI will be used to perform self-inspections.

2.10.1. Forward inspection results in memorandum format, endorsed by the commander to the unit security manager. Security manager will follow-up on any items needing correction or completion.

2.11. End of Day Procedures. End-of-day security checks must be documented on a SF 701, (Activity Security Checklist). Each work area shall establish that the last person leaving the work area will ensure all items listed on the SF 701 are checked and signed off. The SF 701 should be posted near the exit of the room being checked.

2.11.1. Checks should include rooms and areas where classified material can be viewed, stored, processed, copied, printed or faxed to ensure all material is properly removed and secured.

2.11.2. Ensure individuals with at least a SECRET clearance perform end-of-day checks and lockup if classified in the area.

2.11.3. If the work center has security containers (safes, vault doors, open storage areas) include them on the SF 701 Checklist to ensure they are secured. Ensure all windows and doors are locked and all appliances are turned off. All personnel must check their desk and surrounding area for classified material that may have inadvertently been discarded or misplaced during the day.

2.11.4. Individuals working or entering the facility after normal duty hours perform another end of day check prior to leaving the facility. This check will also be annotated on the SF Form 701.

2.12. Secure Telephone Unit-III (STU) keys/ Secure Telephone Equipment (STE) cards.

2.12.1. The terminal is treated as an unclassified, high value item when the Crypto Ignition Key (CIK)/STE card is not inserted. When a CIK/card is inserted into the terminal, the unit must not be left unattended. Unless the STU/STE is located in an area operational 24-hours a day, the CIK/card must be removed and properly secured at the close of each business day.

2.12.2. Storage of CIK/STE. IAW AFI 33-209, paragraph A2.4.4, when the key is stored in the same room as the terminal, store the CIK/card in a GSA-approved security container. If a security container is not available store the CIK/card in a locked cabinet or desk, provided the door to the room containing the STU is locked.

BRUCE L. CURRY, Colonel, USAF
Commander

Attachments:

1. Courier Memorandum
2. Exemption Notification Example
3. Self Inspection Checklist

Designation eines offiziellen Kuriers

1. _____ 4th Air Support Operations Group, Campbell Barracks, Heidelberg, Bundesrepublik Deutschland, ist als Kurier der U.S. Regierung designiert. Wenn aufgefordert, wird er einen offiziellen Ausweis mit der Nummer _____ vorlegen.
2. _____ is/in/Besitz von sensitivem Material, mit folgendem Absender _____ und an _____ adressiert. Jedes Paket ist außen mit der Aufschrift 'OFFICIAL BUSINESS-MATERIAL EXEMPTED FROM EXAMINATION' und der Unterschrift des Unterzeichnenden gekennzeichnet.
3. Die oben namentlich aufgeführte Person, hat genaue Anweisung über den richtigen Umgang und die Verwahrung von sensitivem Material nach IAW DOD 5200.1-R/AFR 205-1.
4. Diese Kurier-Designation kann unter folgender Rufnummer bestätigt werden. Dieser Brief verfällt 2 Jahre von Unterzeichnenden dieses Briefs.

BRUCE L. CURRY, Colonel, USAF
Commander

OFFICIAL BUSINESS**MATERIAL EXEMPTED FROM EXAMINATION****ARTICLE 40****NATO STATUS AGREEMENT**

Subject to any provision to the contrary in the NATO Status of Forces Agreement or in the present Agreement, archives, documents, official mail recognizable as such and property of a force shall be immune from search, seizure, or censorship by the German authorities except where immunity is waived.

ARTIKEL 40

Vorbehaltlich entgegenstehender Bestimmungen im NATO-Truppenstatut oder in diesem Abkommen unterliegenden Archive, Dokumente, als solche erkennbare Dienstpostsendungen und Eigentum einer Truppe nicht der Durchsuchung, Beschlagnahme, oder Zensur durch die deutschen Behoerden, sofern auf die Immunitaet nicht verzichtet wird.

BRUCE L. CURRY, Colonel, USAF
Commander, 4th Air Support Operations Group

OFFICIAL BUSINESS

Atch 2

7 October 2002



Security

4TH AIR SUPPORT OPERATIONS GROUP SECURITY PROGRAM

86 SECURITY FORCES SQUADRON
INFORMATION/INDUSTRIAL SECURITY PROGRAM REVIEW CHECKLIST

Organization Visited: _____ **Date:** _____

Name of Security Manager/Alternate: _____ **Phone:** _____

Personnel Contacted: _____

Personnel Outbriefed: _____

1. PROGRAM MANAGEMENT: (AFI 31-401 & DoD 5200.1-R)

- | | | | |
|---|-----|----|-----|
| A. Are security managers appointed in writing by the unit commander?
(AFI 31-401, para 1.3.5.1. & USAFE Sup, para 1.3.6. (a)) | YES | NO | N/A |
| B. Are security managers trained within 90 days of appointment?
(IC 2000-1 TO AFI 31-401, CHAPTER 8) | YES | NO | N/A |
| C. Does the Security Manager maintain a current OI outlining
the unit's information security program? (AFI 31-401, para 1.3.6.2) | YES | NO | N/A |
| D. Are self-inspections conducted semi-annually? (AFI 31-401, para 1.4.3) | YES | NO | N/A |
| E. Does the security managers attend ISPM security manager meetings?
(AFI 31-401. para 1.3.6.4.) | YES | NO | N/A |

F. Security Education Training Plan: (IC 2000-1 TO AFI 31-401, CHAPTER 8) YES NO N/A

G. Does the security manager maintain the following documents?

(AFI 31-401, USAFE Sup1, para 1.3.6.)

- | | | | |
|---|-----|----|-----|
| (1) Current Sentinel Key roster for assigned civilian and military personnel. | YES | NO | N/A |
| (2) Copy of the last ISPM program review report.
(AFMAN 37-139, Table 31-4, rule 48) | YES | NO | N/A |
| (3) Copy of the last two self-inspection reports (AFMAN 37-15, rule 31) | YES | NO | N/A |
| (4) Copy of the most current security manager meeting minutes.
(AFMAN 37-139, Table 37-11, rule 13) | YES | NO | N/A |
| (5) A list of security containers, vaults, and secure rooms within the organization, including make, container ID number, lock type and location. (AFI 31-401, USAFE Sup1, para 1.3.6. (d)) | YES | NO | N/A |
| (6) AF Form 2587 Debriefing Statements (Retained for 2 years)
(AFI 31-401, para 8.10) | YES | NO | N/A |
| (7) Are personnel authorized to handcarry classified material properly briefed in accordance with DoD 5200.1-R, para 7-300(b)
(AFI 31-401, para 6.7.2.) | YES | NO | N/A |

2. SAFEGUARDING AND STORAGE: (AFI 31-401 & DoD 5200.1-R)

A. Are the following forms available and properly completed?

- | | | | |
|--|-----|----|-----|
| (1) Standard Form 700, "Security Container Information"
(AFI 31-401, para 5.23.2 & DoD 5200.1-R, para 6-404b(2)) | YES | NO | N/A |
| (a) When part II of the 700 is used to record the safe combination, is it marked and protected at the same level as the material stored in the safe? (AFI-31-401, par 5.23.3 –523.3.2) | YES | NO | N/A |
| (2) Standard Form 701, "Activity Security Checksheet"
(DoD 5200.1-R, para 6-302) | YES | NO | N/A |
| (3) Standard Form 702, "Security Container Checksheet"
(DoD 5200.1-R, para 6-302) | YES | NO | N/A |
| (4) Air Force Technical Order Form 36,
"Maintenance Record For Security Type Equipment"
(AFI 31-401, para 5.19 & TO 00-20F-2, para 9b) | YES | NO | N/A |

- | | | | |
|---|-----|----|-----|
| B. Are only GSA approved security containers used for the storage of classified material? (AFI 31-401, para 5.19) | YES | NO | N/A |
| C. Have unit commanders approved areas for open storage of classified Material? (AFI 31-401, USAFE SUP1, para 5.20.4.) | YES | NO | N/A |
| (1) Has the local CE conducted a site survey and determined the facility meets structural requirements as outlined in DoD 5200.1-R, Appendix G. (AFI 31-401, USAFE SUP1, para 5.20.4.) | YES | NO | N/A |
| (2) Does the facility meet all other security criteria for storage of classified material as outlined in DoD 5200.1-R and AFI 31-401? | YES | NO | N/A |
| (3) Is the approval for open storage granted in writing? (AFI 31-401, USAFE SUP1, para 5.20.4.) | YES | NO | N/A |
| (4) If the facility does not meet all DoD and Air Force security requirements for the storage of classified material, has approval of alternative/compensatory security controls been coordinated and approved by 86 SFS/SFAII? (AFI 31-401, para 5.30.1) | YES | NO | N/A |
| D. Do locks used to secure classified storage containers, vaults and and secure rooms meet federal specification FF-L-2740? (DoD 5200.1-R, para 6-402A(3)) | YES | NO | N/A |
| E. Are key operated locks used to secure areas containing bulky secret and confidential material approved by the chief of the activity? (AFI 31-401, para 5.21.1.) | YES | NO | N/A |
| (1) Has the authorizing official designated key and lock custodians? (AFI 31-401, para 5.21.1) | YES | NO | N/A |
| (2) Is AF Form 2427, Lock and Key Control Register used to identify and keep track of keys? (AFI 31-401, para 5.21.2.) | YES | NO | N/A |
| (3) Does the lock meet Federal Specification FF-P-110 for changeable combination padlocks or Military Specification MIL-P-43607 for high security key operated padlocks? (DoD 5200.1-R, para 6-402f) | YES | NO | N/A |
| F. Has an Emergency Protection Plan been developed in accordance with DoD 5200.1-R, para 6-303? | YES | NO | N/A |
| G. Open/Closed Sign displayed (Recommendation) | YES | NO | N/A |
| H. Is access to classified material granted only to those personnel who have a security clearance, need to know and have signed a SF 312, Non-Disclosure Agreement? (AFI 31-401, para 5.4) | YES | NO | N/A |

I. Are cover sheets used for classified that is removed from storage? YES NO N/A
(AFI 31-401, para 5.11.)

3. REPRODUCTION AND DESTRUCTION: (AFI 31-401 & DoD 5200.1-R)

A. Have unit commanders or staff agency chiefs designated equipment for classified reproduction? (AFI 31-401, para 5.26.1) YES NO N/A

B. Is classified reproduction equipment approved by information managers? YES NO N/A
(AFI 31-401, para 5.26.2)

(1) Have information managers issued procedures for clearing copier equipment of latent images? Are these procedures posted? YES NO N/A
(AFI 31-401, para 5.26.2 & 5.26.3.1)

C. Has the security manager developed procedures to ensure control of classified material and ensure personnel understand their security responsibilities during reproduction of classified material? YES NO N/A
(AFI 31-401, para 5.26.3.2 & 5.26.3.3. & DoD 5200.1-R, para 502)

D. Have unit commanders designated personnel by position to exercise reproduction authority for classified material in their activities? YES NO N/A

Is this list posted? (AFI 31-401, para 5.27)

E. Is classified material that has been identified for destruction, protected until it is actually destroyed? (DoD 5200.1-R, para 6-700a) YES NO N/A

F. Are approved shredders used for destruction of classified material? YES NO N/A
(AFI 31-401, para 5.29.1. & DoD 5200.1-R, para 6-701b)
How are shredders labeled? (observation)

G. Is destruction of U.S. classified material accomplished by appropriately cleared personnel? (AFI 31-401, para 5.29.2.-5.29.2.5.) YES NO N/A

4. MARKINGS

A. Are the following labels used to mark AIS storage media and equipment?

(1) SF 706, TOP SECRET AIS media classification label YES NO N/A
(DoD 5200.1-R, para 5-409)

(2) SF 707, SECRET AIS media classification label YES NO N/A
(DoD 5200.1-R, para 5-409)

(3) SF 708, CONFIDENTIAL AIS media classification label (DoD 5200.1-R, para 5-409) YES NO N/A

(4) SF 710, UNCLASSIFIED AIS media classification (DoD 5200.1-R, para 5-409) YES NO N/A

B. Do classified documents possess the following markings

(1) Overall classification on the front cover, title page, first page? and outside of back cover. (DoD 5200.1-R, para 5-200) YES NO N/A

(2) The agency and office of origin? (DoD 5200.1-R, para 5-201) YES NO N/A

(3) The source/s of classification? (DoD 5200.1-R, para 5-202) YES NO N/A

(4) Additional warning notices? (DoD 5200.1-R, para 5-208) YES NO N/A

C. If the unit receives improperly marked classified, do they contact the sender? Is this contact documented? (DoD 5200.1-R, 5-102, b.) YES NO N/A

D. Are the following types of classified material properly marked?

(1) Working papers (DoD 5200.1-R, para 6-101 & AFI 31-401, para 5.3) YES NO N/A

(2) Electronic Messages (DoD 5200.1-R, para 5-307) YES NO N/A

(3) Transparencies/Films/Slides (DoD 5200.1-R, para 5-402 & 5-403) YES NO N/A

(4) Motion Picture Films & Videotapes (DoD 5200.1-R, para 5-404) YES NO N/A

(5) Photographs, Negatives, & Unprocessed Film (DoD 5200.1-R, para 5-402) YES NO N/A

(6) Blueprints, Schematics, Maps & Charts (DoD 5200.1-R, para 5-401) YES NO N/A

(7) Sound Recordings (DoD 5200.1-R, para 5-405) YES NO N/A

(8) Microforms (DoD 5200.1-R, para 5-406) YES NO N/A

(9) Removable AIS Storage Media (DoD 5200.1-R, para 5-407) YES NO N/A

(10) Fixed and Internal AIS Storage Media (DoD 5200.1-R, para 5-408) YES NO N/A

5. NATO CLASSIFIED (AFI 31-406, “Applying North Atlantic Treaty Organization (NATO) Protection Standards”, dated 01 Apr 00.

A. Is NATO Access granted only by personnel designated in writing by the commander or staff agency chief? (para 4.2.)	YES	NO	N/A
B. Are NATO briefings conducted and recorded on AF Form 2583 prior to granting access to NATO classified? (para 4.9.)	YES	NO	N/A
C. Are Annual ATOMAL briefings accomplished? (para 4.9.1)	YES	NO	N/A
D. Are personnel debriefed from NATO access via AF Form 2587? (para 4.10.)	YES	NO	N/A
E. Are combinations to storage containers changed every 12 months? (para 5.3.1.)	YES	NO	N/A
F. As a minimum are file dividers used to separate NATO from all other material? (para 5.1.)	YES	NO	N/A
G. Are file folders marked with the highest classification of the material stored within? (5.1.)	YES	NO	N/A
H. Are COSMIC Top Secret accountability records (AF Form 143) maintained for 10 years? (AFMAN 37-139, TABLE 31-4, RULE 31)	YES	NO	N/A
I. Are COSMIC Top Secret accountability records maintained separately from US Top Secret records? (para 6.5.)	YES	NO	N/A
(1) Are CTSA accountability records kept separate from CTS records? (para 6.5.)	YES	NO	N/A
J. Is the AF Form 144 used to record disclosure of CTS material? (para 5.6.2.)	YES	NO	N/A
K. Are annual audit/inventories conducted of all CTS material by one or more properly cleared and disinterested person/s? (para 5.6.4.)	YES	NO	N/A
L. Are CTS inventory/audit reports endorsed by the sub-registry or control point commander? (5.6.4.1.)	YES	NO	N/A
(1) Do control points send the report to the sub-registry? (para 5.6.4.1.)	YES	NO	N/A
(2) Does the sub-registry send the report to the CUSR? (para 5.6.4.1.)	YES	NO	N/A
M. Is CTS material returned to sub-registry for destruction? (para 5.12.)	YES	NO	N/A

- N. When additional copies of CTS & CTSA documents are needed, are they obtained from the NATO originator? (para 5.11.1.) YES NO N/A
- (1) When not practical to obtain copies from the NATO originator, is authority to reproduce CTS obtained from the sub-registry. For reproduction of CTSA documents, is reproduction authorization obtained from the CUSR? (para 5.11.1.1.) YES NO N/A
- O. Are NATO Secret documents administratively controlled by using either an AF Form 310 or general purpose work sheet. (para 5.8.) YES NO N/A
- P. Are receipts used when sending NATO Secret material outside the unit or Activity? (para 5.8.) YES NO N/A
- Q. Is NATO secret and above destroyed by two appropriately cleared personnel, and documented on the AF Fm 310 (NATO secret) or the AF FM 143 (CTS, CTSA)? (5.12.1. & 5.12.2.) YES NO N/A
- (1) Are destruction records maintained IAW AFMAN 37-139? (NATO secret-2yrs./CTS & CTSA-10yrs) YES NO N/A

6. TOP SECRET CONTROL ACCOUNT (Use checklist provided by USAFE/SFII 12 Jan 00)

CHECKLIST FOR: TOP SECRET CONTROL 12 JAN 00 HQ USAFE/SFII
 COMMENTS

- 1. Is a Top Secret Control Officer (TSCO) designated by the unit commander or staff agency chief at activities that store Top Secret Information? (AFI 31-401, 5.10.1.1) YES NO N/A
- 2. Is an AF Form 143, *Top Secret Register Page*, used to account for all Top Secret documents and AIS material? (AFI 31-401, 5.10.1.1) **NOTE:** TSCO's may automate their accounts as long as all the required information is included. YES NO N/A
- 3. For AIS media, are the contents of the media listed on the AF Form 143 or separate sheet of paper? (AFI 31-401, 5.10.1.1) YES NO N/A
- 4. Does the TSCO use AF Form 144, *Top Secret Access Record and Cover Sheet*, as the disclosure record and keep it attached to the applicable Top Secret material? (AFI 31-401, 5.10.1.2.1) YES NO N/A
- 5. Are inventories on the Top Secret accountability systems conducted every 12 months or when the TSCO changes? (AFI 31-401, 5.10.1.3.1) YES NO N/A
- 6. Are Top Secret facsimiles treated and controlled like reproductions? (AFI 31-401, 5.10.1.5) YES NO N/A

7. When Top Secret is not under personal control is it stored in the following manner? YES NO N/A
(DoD 5200.1-R, 6-402a)
- a. GSA approved security container with supplementary controls.
 - b. Vault or secure room with an IDS.
8. Are two people and a destruction certificate used when destroying Top Secret N/A
information? (AFI 31-401, 5.29.2.1) YES NO
9. Is Top Secret information transmitted only by: (DoD 5200.1-R, 7-101) YES NO N/A
- a. Following established handcarry procedures
 - b. Approved cryptographic system
 - c. Defense Courier Service, Department of State Diplomatic Courier

7. PERSONNEL SECURITY (DoD 5200.2-R and AFI 31-501)

- A. Are positions coded with the proper SAR/ACCESS code? YES NO N/A
(AFI 31-501, para 7.1.2.1.)
- B. Are PR's completed as required? (AFI 31-501, para 3.28.) YES NO N/A
PR backlog progress? Can SM identify disposition of backlogs?
(observation)
- C. Does SM have Sentinel key? (AFI 31-501, para 7.42.) YES NO N/A
- D. Are initial and refresher briefings being conducted on cleared personnel? YES NO N/A
(AFI 31-501, para 9.3.)

8. INDUSTRIAL SECURITY (DoD 5200.2-R, AFI 31-501, AFI 31-601 and VGSA)

- A. Does unit have contractor working for them? If yes, what do they do? YES NO N/A
Is it a classified contract? How many people work on the contract _____
United States Citizens _____ # Foreign Nationals _____
- B. Does the SM process the contractor's personnel security questionnaire if YES NO N/A
access is needed for unescorted entry to restricted areas, access to sensitive
unclassified information, access to government automated information systems
(AIS) and/or sensitive equipment, not involving access to classified information?

(AFI 31-601, para 2.4.1, DoD 5200.2-R and AFI 31-501)

C. Is SM including contractor personnel in initial, refresher and annual training? (AFI 31-601, para 3.1.4., DoD 5200.1-R , AFI 31-401, Chapter 8 and VGSA)	YES NO N/A
--	------------

D. Has the SM established a file with the following documentation? -Signed coy of the DD Form 254 and any revisions -Signed copy of the Visitor Group Security Agreement (VGSA) -Current listing of Key on-base management -Copy of last annual program review -Copies of last two self-inspections reports. The annual program review can be used to substitute for one of the self-inspections. -Copy of all contractors' visit authorization letter (AFI 31-601, para 6.2.4., VGSA)	YES NO N/A
---	------------