

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

AIR FORCE INSTRUCTION 33-211

1 NOVEMBER 1997



AIR FORCE SPACE COMMAND

Supplement 1

3 DECEMBER 2001

Communications and Information

**COMMUNICATIONS SECURITY (COMSEC)
USER REQUIREMENTS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCI (CMSgt Hogan)
Supersedes AFI 33-211, 1 October 1995.
(AFSPC) AFI33-211_AFSPCSUP1, 1 Mar 99.

Certified by: HQ USAF/SCXX (Lt Col McGovern)
Pages: 48
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*; Air Force Systems Security Instruction (AFSSI) 4100, (C) *Communications Security (COMSEC) Program (U)*; and AFKAG-1, *Air Force Communications Security (COMSEC) Operations*. It outlines responsibilities and clarifies procedures for the communications security (COMSEC) responsible officer (CRO) and COMSEC users to properly secure COMSEC material the local COMSEC manager issued to them. Refer technical comments to Headquarters Air Force Communications Agency (HQ AFCA/GCI), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5218. Refer recommended changes and conflicts between this and other publications on an AF Form 847, **Recommendation for Change of Publication**, through channels, to HQ AFCA/XPPX, 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5233. Major commands (MAJCOM), field operating agencies (FOA), and direct reporting units (DRU) send one copy of final supplement to HQ AFCA/XPPX. This instruction applies to all users who receive COMSEC material from Air Force COMSEC channels. See Attachment 1 for a glossary of references, abbreviations, acronyms, and terms.

(AFSPC) The OPR for this supplement is AFSPC CSS/SCOI (Mr. David S. Samp). This supplement implements and extends the guidance of Air Force Instruction (AFI) 33-211, *Communications Security (COMSEC) User Requirements*. The AFI is published word-for-word without editorial review. Air Force Space Command (AFSPC) supplemental material is indicated in bold face. This supplement describes AFSPC's procedures for use in conjunction with the basic AFI. It applies to AFSPC COMSEC accounts and organizations supported by the AFSPC Communications Support Squadron, 150 Vandenberg St., Ste 1105, Peterson AFB CO 80914-4730. This publication applies to all Air Force Reserve Command (AFRC) and Air National Guard (ANG) units assigned to AFSPC. Upon receipt of this integrated supplement discard the Air Force basic publication.

SUMMARY OF REVISIONS

Clarifies and updates guidance for COMSEC users.

SUMMARY OF REVISIONS

(AFSPC) Clarifies and updates guidance for COMSEC users. This publication incorporates 33 AFSPC recommended changes to provide specific information not contained in the basic publication. A bar (|) indicates a revision from the previous edition.

Section A—General Instructions

1. Introduction. This AFI sets procedures for CROs and COMSEC users. It describes their COMSEC duties and the minimum requirements for safeguarding, controlling, and destroying COMSEC material routinely and during an emergency. Controls apply to accessing, using, producing, developing, moving, storing, accounting for, and disposing of COMSEC material. This AFI also describes the two-person integrity (TPI) policy and procedures for all Top Secret COMSEC key and Top Secret key-generating equipment. It contains general COMSEC information of interest to all CROs and COMSEC users who receive COMSEC aids.

2. Objective. This AFI provides CROs and COMSEC users with detailed procedures for protecting and safeguarding COMSEC material.

Section B—Management and Responsibilities for Communications Security Material

3. Authorizing the Receipt and Transport of Communications Security Aids. The authorizing official of each section that needs COMSEC aids appoints, by letter, a primary CRO and at least one alternate to receive material from the COMSEC account (see [Attachment 2](#)). The letter includes each individual's name, rank, social security number (SSN), security clearance (including North Atlantic Treaty Organization [NATO] access), duty telephone, and locations the individuals may carry COMSEC aids to and from. The CRO and alternates carry copies of the letters when they transport COMSEC aids. The authorizing official updates this letter to reflect changes as they occur.

3.1. Persons appointed as primary CROs must have a minimum grade of staff sergeant or General Schedule (GS)-5. Alternates must have a minimum grade of senior airman or GS-4. Wage Grade personnel normally do not perform administrative responsibilities; however, when appointment is necessary, administrative responsibilities will be comparable to GS-5 for CRO or GS-4 for alternate CRO. Appoint foreign nationals as CROs, provided they hold only material that is releasable to their country. They must hold comparable grades required of United States (U.S.) personnel. The local unit commander must approve waivers for personnel with lower grades. Process waivers through the COMSEC manager.

3.2. Make sure CROs are trained by the COMSEC manager and know they are accountable for the material they receive. When a CRO transfers, make sure another CRO or alternate signs for COMSEC aids. Contact the COMSEC manager for approval to transfer COMSEC aids and to prepare new hand receipts.

4. Communications Security Responsibilities:

4.1. COMSEC Manager. The local COMSEC manager:

4.1.1. Receives all COMSEC aids intended for issue to CROs, issues all COMSEC material on Standard Form (SF) 153, **COMSEC Material Report**, and instructs CROs and alternates, in writing, how to use, control, and store the material.

4.1.2. Audits and inventories users accounting legend codes (ALC)-1 and ALC-2 COMSEC material control system (CMCS) holdings.

4.1.3. Provides guidance on setting up CRO functions.

4.1.4. Gives CROs information on effective dates, supersession dates, compromise information, and physical security requirements for operational systems before issuing COMSEC material.

4.1.5. Enters the required status information on the Air Force Communications Security (AFCOMSEC) Form 21, **Disposition Record for KI-1B/C Keytapes**; AFCOMSEC Form 22A, **Disposition Record for Single Copy Keytapes (Except KI-1B/C)**; AFCOMSEC Form 22B, **Disposition Record for Multicopy Keytapes (Except KI-1B/C)**; or on the front covers before issuing COMSEC aids.

4.1.6. Ensures CRO and alternate CRO receive training. Use this AFI and other applicable publications to set up an effective training program. **NOTE:** Use AFCOMSEC Form 30, **COMSEC Responsible Officer and User Training Checklist**, to document initial training of all CROs, alternate CROs, and users.

4.2. Commander. The commander of each unit that needs COMSEC aids:

4.2.1. Makes sure the authorizing official names, in writing, a CRO and at least one alternate to receive COMSEC aids.

4.2.2. Makes sure adequate, approved security containers or facilities are available for storing COMSEC aids.

4.2.3. Takes immediate, corrective action in response to discrepancies identified during a command COMSEC functional review or a base COMSEC manager semiannual functional review. All functional review reports require the commander's action or endorsement.

4.2.4. May appoint more than one CRO in large units, depending on the number of COMSEC users and the volume of material handled.

4.2.5. Makes sure a National Security Agency (NSA) approved destruction device is readily available.

4.3. CROs:

4.3.1. Notify the COMSEC manager, in writing, of any new requirements or changes (increase or decrease) to existing requirements (see [Attachment 3](#)).

4.3.2. Review annually the requirement for COMSEC material, assessing the validity of each item, and in turn provide the COMSEC manager, in writing, the complete list of your COMSEC requirements to include the quantity, purpose, and, or authority (i.e., plan, regulation, operation order, etc.) for each item.

4.3.3. Make sure all persons granted access to COMSEC aids have the proper clearance and a valid need to know by comparing those listed on the access list to the local automated security clearance approval system (ASCAS) roster.

4.3.4. Keep an accurate list of persons with authorized access to COMSEC holdings (see Attachment 4). Use Air Force (AF) Form 1109, **Visitor Register Log**, or Federal Aviation Administration (FAA) Form 1600-8(for FAA accounts) to report access by persons not on the list. For COMSEC users located in controlled facilities, keep a separate visitor's log to record access to the COMSEC material. Verify monthly, by date and initials, the final clearance of all personnel on the access list.

4.3.5. Set up a comprehensive, periodic training program to make sure all personnel with authorized access know how to handle, control, and use the material. Ensure all personnel are familiar with correct procedures in operating associated cryptographic equipment using applicable AFKAOs, KAOs, or similar instructions provided by the COMSEC manager. Conduct initial training and use AFCOMSEC Form 30 to document it. Complete a separate training checklist for each person with access. Provide annual refresher training to all personnel who have been granted access. Record the date, subjects covered, and persons trained. Keep training documentation from command functional review to command functional review.

4.3.5. (AFSPC) The CRO and COMSEC manager must identify which training areas on the AF Form 4168, COMSEC Responsible Officer and User Training Checklist, pertain to the specific user. These training areas will become mandatory for those users. Individuals will not be granted unescorted access until initial training is accomplished and properly documented on the AF Form 4168.

4.3.5.1. (Added-AFSPC) Annual training will be documented on the AF Form 4168 and will include all training areas identified in paragraph 4.3.5. (AFSPC).

4.3.5.2. (Added-AFSPC) Users that have 25 or more persons on their access list may be exempt from using the AF Form 4168 to document annual training. Minimum required documentation is a completed AF Form 4168. The trainer must initial all blocks appropriate for that sub-account and/or group of users. Other tasks/requirements may be added to the AF Form 4168 or maintained as a separate but attached document. A separate form containing the printed/typed names and signatures of both the trainer and the trainee and the date the training was conducted must be attached or available for review.

4.3.5.2.1. (AFSPC) The method used for documentation of training must be specifically outlined in a local Operating Instruction (OI) appropriately coordinated through the COMSEC manager.

4.3.5.3. (Added-AFSPC) Use of Core Automated Maintenance System (CAMS) to document training is not authorized.

4.3.6. Take responsibility for receiving, accounting for, checking pages of, handling, using, and safeguarding all CMCS material they or their alternate receives until it is destroyed or returned to the COMSEC account. Per direction of the COMSEC manager, maintain an exact copy of the hand receipt maintained at the COMSEC account for all material received and the CRO has taken responsibility.

- 4.3.7. Develop a local operating instruction (OI) on handling, controlling, and protecting COMSEC assets, including inventory, TPI (if applicable), destruction, COMSEC incident reporting, and a requirement for CROs and secure telephone unit (STU) responsible officers (SRO) to get the COMSEC manager's clearance from responsibility before leaving their current assignment. COMSEC users must clear through their CRO and SRO. Coordinate the OI with the COMSEC manager.
- 4.3.8. Perform inventories per paragraph 19.
- 4.3.9. Verify COMSEC materials are inventoried according to their respective ALC.
- 4.3.10. Carry out duties the COMSEC manager requires, such as performing page checks, etc.
- 4.3.11. Issue COMSEC materials to user activities per this instruction, when applicable.
- 4.3.12. Give a receipt to transient personnel who turn in material for safekeeping. When the person reclaims the material, retrieve the receipt for the material from the transient personnel. Your accountability for the material ends.
- 4.3.13. Return or destroy all material as the COMSEC manager directs. Destroy COMSEC aids per Section E.
- 4.3.14. Keep all records according to Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339).
- 4.3.15. Develop an emergency action plan (EAP) that consists of task cards; coordinate it with the COMSEC manager and conduct EAP training per Section G.
- 4.3.16. Use a checklist to ensure completion of required security checks.
- 4.3.17. Provide an update report every 60 days on findings identified during functional reviews, or as the COMSEC manager directs, until they are corrected.
- 4.3.17. (AFSPC) **Provide an update report on findings identified during functional reviews, as the COMSEC manager directs, or at least every 60 days until corrected and closed by the COMSEC manager. Reporting should not be delayed for internal coordination.**
- 4.3.18. Report all known or suspected COMSEC incidents to the COMSEC manager.
- 4.3.19. Familiarize all personnel who are granted access with applicable Air Force publications and specialized COMSEC publications (e.g., OIs, AFI 33-211, KAMs, KAOs, etc.) semiannually.
- 4.3.19. (AFSPC) **Document this familiarization as "Required Reading" and specifically identify the reviewed publications. Minimum documentation to be maintained is: what publications were read; when the reading was accomplished; and trainees signature certifying that they completed the reading.**
- 4.3.20. Enroll all applicable personnel in the cryptographic access program (CAP) as outlined in AFI 33-210, *Cryptographic Access*, and remove them from the CAP when they are removed from the access list.
- 4.4. COMSEC Users. COMSEC users have access to COMSEC aids and the responsibility for safeguarding them. COMSEC's ultimate success or failure rests with the material's individual users. The careless user or the user who fails to follow procedures for using, safeguarding, and destroying COMSEC material wastes all security efforts. COMSEC users must make sure that anyone who receives

materials has authorization. Users must follow all security rules at all times and report to the CRO or the COMSEC manager any circumstances or intentional or inadvertent acts that could lead to disclosure of classified information, including its loss, improper use, unauthorized viewing, or any other instance that could possibly jeopardize the value of COMSEC aids. COMSEC users:

- 4.4.1. Safeguard COMSEC material according to this document and control the material locally until they destroy it or turn it in.
- 4.4.2. Return material to the CROs on request.
- 4.4.3. Familiarize themselves with correct procedures for operating associated cryptographic equipment and devices using applicable AFKAOs, KAOs, or instructions provided by the CRO.
- 4.4.4. Report immediately any known or suspected compromise of COMSEC material to the CRO or COMSEC manager as instructed by AFI 33-212, *Reporting COMSEC Incidents*, and paragraph 53.

5. Producing Communications Security Aids. Only the NSA and the services cryptology elements are authorized to produce nomenclature and non-nomenclature COMSEC aids. Other Air Force activities must not originate, formulate, or produce keylists, codes, ciphers, callsigns, authenticators, or any other form of COMSEC aids. Do not remove, copy, or reproduce any part of COMSEC keying material unless the authority controlling the material permits it or it's authorized in the material's handling instructions. Other activities may make extracts from general publications when authorized in the document's handling instructions.

6. Requesting Communications Security Material. CROs tell the COMSEC manager, by letter, what COMSEC aids they need to support the mission (see [Attachment 3](#)).

- 6.1. Emergency requests (less than 60 days notice before the required in-place date) must include a fund citation from the requesting unit to cover shipping and transportation costs.
 - 6.1.1. (Added-AFSPC) **The requesting unit may be tasked to provide courier personnel to meet the emergency requirement.**
- 6.2. Process requests for most COMSEC equipment through the standard base supply system (SBSS). Send a COMSEC material requirements letter to the COMSEC manager at the same time to make sure COMSEC material is on hand when required. When in doubt contact the COMSEC manager for direction.

7. Authorized Access. Only U.S. citizens, whose official duties require it, may access keying material and equipment, except those specifically authorized for release to allies. Certain material and equipment may require enrollment in the CAP. Contact COMSEC account personnel for details of CAP needs.

- 7.1. For keying material, persons must have a security clearance equal to or higher than the classification level of the keying material involved.
- 7.2. For keyed or unkeyed equipment, persons must have a security clearance equal to or higher than the classification level of the equipment or of the keying material, whichever classification is higher.
- 7.3. For Top Secret keying material, Section F applies.

8. Issuing to Communications Security Users. In general, keying material must remain under the COMSEC manager's control until issued and the CRO's control until just before its effective period.

8.1. Normally issue users no more than one month's supply of material; however, if a user needs more for an active mission, the COMSEC manager issues sufficient COMSEC aids to meet the need, but not more than 120 days worth.

8.2. Except for special circumstances, do not issue users a new month's material more than 10 duty days before its effective date.

8.3. You may issue complete canisters of key for use on aircraft; however, all unused key must be returned to the issuing CRO upon mission completion. Prior to issue:

8.3.1. Page check and seal documents (i.e., code books, authenticators, etc.). Issue the sealed document and disposition record to the aircrew in its entirety. If the sealed document is not used, or if used during the flight and no pages or tables have been removed, the aircrew will return the entire document to the issuing CRO. Once single/multiple tables/pages are removed from the document, the aircrew must destroy these items not later than 12 hours after supersession and annotate this destruction on the disposition record.

8.3.2. Issue keytape canisters in their entirety to include its associated disposition record or appropriate form. Before issuing key canisters, the CRO will remove and destroy all superseded material. Aircrew members must destroy any keytape segments removed from the canister within 12 hours after supersession and record this destruction on the associated disposition record. Segments remaining in the canister need not be removed for destruction and will be returned to the issuing CRO.

8.3.3. Issue material in a COMM kit that can be sealed for turn-in at remain overnight (RON) locations. Design the kit to ensure that the seal will prevent unauthorized access and that any tampering would be evident. Aircrews must inventory all material prior to sealing the kit for turn-in. Ensure personnel manning storage locations at RON location are instructed to retain the sealed kit (RON storage locations will sign "only" for the sealed kit via AF Form 12, **Accountable Container Receipt**, etc.) and reissue it to the same crew. RON storage locations are not to reissue material to other aircrews/aircraft. (See paragraph 19.5 for additional instructions.)

8.3.4. Must make sure users maintain strict accountability and destroy superseded keys within established time frames. When issuing ALC-1 COMSEC aids directly to transient or special purpose aircraft aircrews whose mission makes it probable they will not return the material, disposition record, or destruction certificates to the issuing office, annotate the receipt (SF 153 or AFCOMSEC Form 1, **COMSEC Users Receipt/Destruction Certificate**) with the following statement: "I FULLY UNDERSTAND THE RULES FOR THE PROTECTION AND PROPER DESTRUCTION OF THE ABOVE MATERIAL INDICATED ON THIS HAND RECEIPT, ACCORDING TO AFI 33-211." The CRO files and keeps the properly completed receipt with the destruction certificates. This is a procedure commonly referred to as "presumed destruction" and pertains only to transient and special purpose aircraft. The Air Force still expects transient and special purpose aircraft aircrews to properly handle, protect, and destroy COMSEC aids even though they do not tell the issuer how they disposed of them. **NOTE:** Deploying aircrews who receive COMSEC material from their CRO must provide disposition and destruction records, along with any unused COMSEC material, to their CRO upon return to home station.

8.4. Extended aircraft missions may require more keying material than the handling instructions permit, particularly if restocking en route is impractical.

8.4.1. Aircrews may carry complete canisters of keytapes or keylists (current plus three months' supply) on board. If a flight begins during the effective period of the canister, remove and destroy superseded settings or segments so you take only the effective and future key settings or segments on board. Users must destroy each key setting within 12 hours after supersession provided destruction facilities are available. If destruction facilities are not available, hold superseded material until the aircrew arrives at a location where they are available.

8.5. Aircrews must make every effort to destroy and record destruction of obsolete material during intermediate stops. If destruction facilities are not available, hold superseded material until the aircrew arrives at a location where they are. Destruction facilities are normally available at secure storage facilities such as base operations, base communications centers, and command posts. This process will result in a significant decrease in the amount of destruction required by aircrews, making accountability much easier, and should reduce the possibility of lost material.

Section C—Administrative Security Procedures

9. Communications Security Forms . Air Force Index (AFIND) 9, *Numerical Index of Departmental Forms*, lists forms used to satisfy COMSEC needs. Contact the local publications distribution office (PDO) for forms. Use of computer-generated AFCOMSEC forms is acceptable.

10. Records Maintenance and Disposition.

10.1. Do not mix COMSEC aids with administrative correspondence or other non-COMSEC documents. As a minimum, use a file folder as a divider between these types of documents.

10.2. Dispose of all records per AFMAN 37-139. This requirement does not permit administrative or security personnel to inspect any COMSEC or COMSEC users' records.

10.2.1. Limit access to these records and files to those persons who manage, administer, operate, and maintain COMSEC aids and equipment.

10.2.2. During records maintenance and administrative staff assistance visits and program management reviews, reviewers may only check the Records Information Management System produced file plan. Do not grant reviewers access to COMSEC materials, records, or files.

10.3. Do not use correction fluid or correction tape on COMSEC records that affect control and accountability of material.

11. Standard Accounting Legend Codes. The originating agency assigns ALC numbers to COMSEC material to identify the minimum accounting controls the material requires.

11.1. ALC-1 material is continuously accountable by accounting number within the CMCS. When removed from an authorized security container, the material must be under the personal control of a cleared person. Do not release this material to any person or organization without the COMSEC manager's consent. Handle unclassified keying material marked **CRYPTO** like other ALC-1, except store it in the most secure place available (i.e., in an approved safe, locked file cabinet, locked desk, locked container, etc.). Always store classified ALC-1 keying material in an approved, locked container.

11.1.1. Use AFCOMSEC Form 16, **COMSEC Account Daily-Shift Inventory**, to make a sight inventory by short title, edition, accounting control number (ACN), and quantity, per paragraph 19.

11.1.2. Return material when the COMSEC manager asks and destroy it only in an emergency or as the COMSEC manager directs, except for issues to transient or deploying aircrews.

11.1.3. Ask the COMSEC manager, in writing, for additional copies of the material per paragraph 8. **NOTE:** Safeguard and account for ALC-1 controlled cryptographic item (CCI) equipment when you receive it from the CMCS on the AFCOMSEC Form 16. Conduct inventories on CCI equipment received from the SBSS according to AFMAN 23-110, *USAF Supply Manual*.

11.2. ALC-2 material is continuously accountable by quantity within the CMCS. Control this material like ALC-1, except inventory by quantity rather than ACN.

11.3. Unless directed by the base COMSEC manager, ALC-4 material does not need to be inventoried. Protect ALC-4 material marked **FOR OFFICIAL USE ONLY** against unauthorized access, use, or possession. Classified ALC-4 material is protected commensurate with its classification level. Give only persons with a need to know access. When ALC-4 material is no longer needed, notify the COMSEC manager in writing.

11.3.1. (Added-AFSPC) **If the COMSEC Manager requires Accounting Legend Code (ALC)-4 material to be inventoried, document the requirement in the local OI.**

12. Status Information. A COMSEC key's short title, alphabetical edition designator with its effective date is classified per AFMAN 33-272, (S) *Classifying Communications Security and TEMPEST Information (U)*. Never reveal it in unclassified correspondence. Report violations through the unit security manager as an information security incident.

Section D—Physical Security Requirements for Communications Security Operations

13. Physical Security Requirements. The Air Force does not prescribe construction of special areas for storing and using COMSEC material. However, areas where COMSEC is used must meet the storage and other physical security requirements for the particular classification level of the COMSEC material (see DODR5200-1WC1-2, DoD Information Security Program Regulation, June 1986; and AFI 31-401, *Managing the Information Security Program*). All activities that use COMSEC materials must practice good operations security.

14. Access Controls and Procedures. CROs must only give persons with appropriate clearance and the need to know access to COMSEC material.

14.1. Set up controls to deny unauthorized persons access. Facilities with the locked-door system must challenge and identify persons before they enter. If guards are assigned, station them immediately outside the entrance. Regardless of the control system, entry procedures must identify persons seeking entry so they cannot view COMSEC activities before entering.

14.2. Limit unrestricted access to COMSEC material in a user facility to persons named on an officially published access list (see [Attachment 4](#)). The list must contain the names and clearance levels of all persons who have COMSEC responsibilities in the facility, and should include the unit commander and supervisors. All personnel on the list must have a clearance equal to or higher than the

COMSEC information to which they have access. Refer to AFI 31-501, *Personnel Security Program Management*, for processing of security clearances.

14.3. Verify personal clearance status from the ASCAS roster, and that the person's need to know exists. CROs must review the authorized access list monthly to ensure its accuracy and then mark the review date and their initials on the list. **NOTE:** The authorizing official (for FAA, Facility Manager) or CRO sign the authorized access list. Get security clearance information for civilian personnel (including DoD and civil agency contractors) from the base security police office or other knowledgeable security offices.

14.3.1. (Added-AFSPC) Note: Contractors do not have access to an Automated Security Clearance Approval System (ASCAS) roster or Sentinel Key, and should retrieve monthly clearance verification through their company security manager or Facility Security Officer (FSO).

14.4. Identify persons on the authorized access list who may authorize access to persons not on the list. Keep the number of persons authorized to admit others to a minimum.

14.5. Record the arrival and departure of all persons not named on the authorized access list, using AF Form 1109 or FAA Form 1600-8 (for FAA use only). For COMSEC users in controlled areas, keep an additional separate visitor register to record access to COMSEC material. Keep the current plus the previous 3 months of AF Form 1109 or FAA Form 1600-8 (for FAA use only) on file.

15. Over-The-Counter Service. COMSEC accounts provide only over-the-counter service. They neither deliver nor permanently store materials for which users have established valid requirements. Users must have their own adequate storage facilities (e.g., approved security container, vault, etc.) and take responsibility for storing and accounting for material not later than one duty day before COMSEC aids' effective date.

16. Storing Communications Security Information and Material. "Storage" as used here means using security containers, vaults, alarms, guards, etc., to protect classified COMSEC information and material during non-working hours or when authorized personnel do not directly and continuously control it. Some security containers or vaults may have been drilled open and then repaired. You may use containers that have been repaired and inspected for safeguarding capabilities (Technical Order [TO] 00-20F-2) to store COMSEC material.

16.1. COMSEC Material. All users who have classified COMSEC material must have immediate access to an authorized storage container to secure the material in case of area evacuation. Store COMSEC material as follows:

16.1.1. Top Secret:

16.1.1.1. A General Services Administration (GSA)-approved, Class 6 and above, steel security container from the Federal Supply Schedule.

16.1.1.2. A Class A vault.

16.1.1.3. An area under continuous surveillance by guards.

16.1.2. Secret:

16.1.2.1. Same as paragraph [16.1.1](#).

16.1.2.2. In a Class B vault.

16.1.3. Confidential:

16.1.3.1. Same as paragraphs **16.1.1.** or 16.1.2.

16.1.3.2. In a secure room.

16.1.3.2.1. (Added-AFSPC) **In a secure room which has been approved for open storage of classified.**

16.1.3.3. Minimally, in a standard field safe.

16.1.4. Unclassified Crypto:

16.1.4.1. Same as paragraphs 16.1.1, 16.1.2, or 16.1.3.

16.1.4.2. In the most secure place available (i.e., locked cabinet, locked desk, etc.).

16.2. Cryptographic Equipment and Components. When classified equipment and components are not installed in an operational configuration, store them in the most secure storage available. As a minimum, store it as required for non-COMSEC material of the same classification (see AFI 31-401). When no authorized person keeps or continuously watches unclassified cryptographic equipment, protect it by:

16.2.1. Storing unclassified equipment to prevent any reasonable chance of theft, sabotage, tampering, or unauthorized access.

16.2.2. Not storing cryptographic equipment or fill devices (KYK-13s or KYX-15s) in a keyed condition. When necessary to store it in a keyed condition, protect it at the same level as the key it contains and place it on the COMSEC inventory. See AFSSI 3021, (FOUO) *Interim Operational Security Doctrine for the AN/CYZ-10/A Data Transfer Device (DTD)(U)*, and AFKAO-10 for data transfer device (DTD) instructions.

16.2.2. (AFSPC) **For fill devices (i.e. KYK-13, KYX-15) without an internal audit trail: The short title and edition of the key stored therein must be written on or attached to the device. When keyed, protect at the classification level of the key set on the device and inventory individually IAW procedures for the ALC of the material.**

16.2.3. Protect unkeyed CCI equipment that is not in a secured facility so, in the unit commander's judgment, there is no reasonable chance of theft, sabotage, tampering, or unauthorized access. When keyed, protect such equipment to prevent its unauthorized use or extraction of its key.

16.2.3.1. (Added-AFSPC) **Mechanical fill devices, including permuter plugs and permuter trays (i.e., KOK-3), will be protected as follows: When unkeyed, protect at the classification marked on the item and inventory by quantity IAW procedures for ALC-2 material. When keyed, protect at the classification of the key set on the device and inventory individually IAW procedures for ALC-1 material. Label each device and list each item on the AFCOMSEC Form 16.**

16.2.3.3.1. (AFSPC) **Each mechanical device must be conspicuously marked to indicate the short title and edition of the key stored therein, which will be written on or attached to the device.**

16.2.3.3.2. (AFSPC) **List each mechanical device on the AFCOMSEC Form 16 by placing (for example) “KOK-3/USKAK-1234 AB” in the “Short Title” block; “1” in the “Quantity” block; and the serial number of the device in the “Serial Number” block.**

16.3. Other COMSEC Material. Safeguard material other than those that paragraphs 16.1. and 16.2 identify (i.e., KAMs, KAOs, SAMs, crypto ancillary material), like other national security information of the same classification. Allow access to those who need to know. **WARNING:** Do not store funds, weapons, controlled substances (drugs), precious metals, safe combinations, or duplicate keys to containers that store these items, in any storage container with classified COMSEC material. Because these items are targets for theft, COMSEC material would be at increased risk.

16.4. Lock Combinations:

16.4.1. Change the lock combinations of security containers used for classified COMSEC material storage:

16.4.1.1. At least once a year (every 6 months for NATO, International Pact Organization, and Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 3260.1, [S] *Policy Governing JCS material[U]*).

16.4.1.2. When a person who knows combinations no longer has access to the containers for any reason other than death.

16.4.1.3. When a container certified as locked is found open.

16.4.1.4. When the combination is compromised.

16.4.2. Classify the safe combination equal to the highest level of classified material you are authorized to store in it.

16.4.3. Store and file safe combinations by:

16.4.3.1. Completing SF 700, **Security Container Information, per the instructions.**

16.4.3.2. Choosing a location that allows ready access in an emergency but is restricted to persons with proper clearance and the need to know. You need not record combinations with administrative Top Secret control since they are controlled within COMSEC channels. Do not store lock combinations in contingency communications facilities.

16.4.4. For each vault or container used to store classified material:

16.4.4.1. Complete an Air Force Technical Order (AFTO) Form 36, **Maintenance Record for Security Type Equipment.**

16.4.4.2. Assign an identification number or symbol. Clearly label the vault or container with the number or symbol.

16.4.4.3. Attach an SF 700 to the inside of the locking drawer of each GSA-approved container or vault.

16.4.4.3.1. (Added) For safes or vaults having more than one lock, prepare an SF 700, Security Container Information, for each lock. For safes or vaults having an electronic lock using the dual access mode, prepare an SF 700 for each combination.

16.4.4.4. Attach an SF 700 to the inside of each drawer of the non-approved GSA container.

Develop an OI describing the proper procedures for locking and checking non-approved GSA security containers.

16.5. Entry Control Devices (Cipher Locks). Use this device only for convenience. It offers no protection from forced entry or surreptitious manipulation. Give the combination only to persons with regular duties in the area. Change cipher lock combinations used to limit access to COMSEC material at least monthly.

17. Security Checks. A required security check at the end of each work day (or beginning of each shift for 24-hour operations) ensures proper storage and safety of all classified COMSEC material. COMSEC users must keep a list of items to be checked or tasks to be done during security checks. During the required security checks, make sure:

17.1. All COMSEC material is properly safeguarded.

17.2. Physical security systems or devices (e.g., door locks, vent covers, etc.) work.

17.3. Safes, locking devices, outer doors, windows, etc., are locked.

17.4. Alarms are set:

17.5. Perform daily security checks in areas containing:

17.5.1. Classified installed or stored COMSEC equipment.

17.5.2. Continuously keyed COMSEC equipment not continuously manned (except part-time stations using over-the-air rekeying).

17.5.3. Material from COMSEC accounts in high risk environments (see AFKAG-1).

17.5.4. Contingency communications facilities do not need daily checking; however, inspect them every 30 days to confirm their integrity and to remove superseded or extraneous material.

17.6. Record the security check on SF 701, Activity Security Checklist; Department of Defense (DD) Form 1753, **Master Station Log**; or use an AF Form 2519, **All Purpose Checklist**.

Section E—Safeguarding and Controlling

18. Operating Instructions. Each CRO must write a COMSEC OI and coordinate it with the COMSEC manager. The OI contains provisions for securely conducting COMSEC operations and for safeguarding COMSEC material. The procedures and instructions in the OI are specific to the user's activity. They should include procedures for cryptographic operations, local accountability for COMSEC material, COMSEC maintenance support, access restriction, storage, routine and emergency destruction, incident reporting, and procedures for relieving people who have received COMSEC material from accountability when they are reassigned.

19. Inventory and Accounting Requirements.

19.1. All user activities with ALC-1 and ALC-2 material must conduct daily or shift inventories per ALC requirements. (See paragraph 11. for detailed explanation of ALCs.)

19.2. Account for all items from date of receipt until date of destruction or return to the COMSEC account.

19.2.1. Only blue or black ink will be used to make entries on the inventory (AFCOMSEC Form 16). Do not use “whiteout”, correction tape, or erasures. Neatly line through, initial, and date errors. Record explanatory remarks on the back of the form.

19.3. Use AFCOMSEC Form 16 to record daily, shift, or other local inventories. Record the short title, edition, quantity, and ACN of each accountable COMSEC item.

19.3.1. (Added-AFSPC) **Mark each page of every inventory with security container identification.**

19.4. Inventory the items listed and indicate on the form that the inventory is complete. The inventory includes accounting for individual segments, tapes, tables, etc., by checking the material on hand against disposition and destruction records.

19.5. For items that are continually issued outside the CRO’s responsibility and then returned at a later date (e.g., combat crew comm, base operations issuing to aircrews, etc.), annotate the AFCOMSEC Form 16 one of two ways:

19.5.1. Completely remove the item from the inventory and when returned, annotate this return as a new entry on the inventory.

19.5.2. Indicate that this material is temporarily out of the CRO’s responsibility and was issued to another responsible person, that an active hand receipt is on file, and that they will return this material to the control of the CRO before end of month (EOM) destruction or supersession by indicating the mark (i.e., D=deployed, I=issued, etc.). When the material is returned to the CRO, resume normal marking (i.e., X). When using this method, list items individually on the inventory by short title, edition, and ACN (one item per line entry).

19.5.3. In either case, users must document inventories on a separate AFCOMSEC Form 16 when COMSEC material is out of the CRO’s control in excess of one day. Provide inventories to the CRO upon mission completion.

19.6. Place disposition records for used ALC-1 material on daily or shift inventories until you return them to the COMSEC manager or transcribe the information to a local destruction report. Keep the current and the previous 6 months of inventory records on file according to AFMAN 37-139.

19.7. For daily operations, inventory COMSEC material in locked or sealed containers on days when you open the containers. Prepare a separate inventory for each COMSEC container. List the material stored in the container on AFCOMSEC Form 16 and inventory the material just before you lock the container for the final time that day. In this way, you account for all COMSEC material when the containers are locked.

19.8. For facilities where security containers remain open around the clock, the oncoming shift conducts an inventory before relieving the shift on duty. List the material required on a shift-to-shift basis on a separate inventory from material required daily. Prepare as many separate inventories as necessary and divide the inventories by operational and functional areas.

19.9. Part-time facilities perform an inventory on opened safes upon opening and before closing the facility.

19.10. Sealed packages containing COMSEC aids must also contain an AFCOMSEC Form 16 identifying each item (locked boxes such as tool boxes, tackle boxes, etc., are not sealed packages). Write the short title and edition of the contents on the outside of the package, number the package, and record

it on AFCOMSEC Form 16. Write the CRO's initials over the package's seal in such a way that tampering will be obvious.

19.10. (AFSPC) Mark the sealed package with the appropriate classification. Place the original AFCOMSEC Form 16 inside the sealed package just prior to sealing. Place the date the package was sealed on the outside of the package along with the signature of the person sealing the package.

19.10.1. (Added-AFSPC) When sealed packages are opened, the material inside must be inventoried using a valid AFCOMSEC Form 16.

19.10.2. (Added-AFSPC) Retain the AFCOMSEC Form 16 from the sealed packages, keep the current and the previous 6 months of inventory records on file according to AFMAN 37-139, *Records Disposition Schedule*. It is not necessary to generate AFCOMSEC Form 16(s) for months the package was not opened. Do not open a sealed package for the sole purpose of taking an inventory.

19.11. On an AFCOMSEC Form 16, inventory classified and, or certified (e.g., KG/KT-83, KOK-13) COMSEC equipment received from the COMSEC account through the CMCS. On a daily or shift-to-shift basis, account for operational cryptographic equipment (rack-mounted in the operating area) that contains accountable components or items as one complete unit without viewing the interior.

19.12. Inventory PROMs (programmable read-only memory) (crypto material in the form of chips) any time the locking bars or seals are removed from the equipment.

19.13. The CRO must review inventories monthly to make sure they are accomplished correctly. Document the reviews by initialing the AFCOMSEC Form 16.

19.14. Do not open material in protective packaging (i.e., aids sealed in plastic or keytapes in canisters) or contained in edge-sealed, one-time pads for page checking or inventory of contents.

19.15. (Added-AFSPC) Unkeyed mechanical devices (i.e., KOK-3) will be inventoried as ALC-2. Keyed mechanical devices must be inventoried as ALC-1 and listed on the AFCOMSEC Form 16. Also, refer to para 16.2.3.

20. Page Checks of Classified Communications Security Publications.

20.1. To protect the integrity of COMSEC aids, you must check pages of classified COMSEC publications:

20.1.1. Before initial issue to any aircrew.

20.1.2. When you receive single copies of editions of material from the COMSEC account and cannot get a replacement copy sufficiently before the effective period (e.g., aircrews, remote sites, etc.). Check that the document does not have printing or production errors. Report errors to the COMSEC manager.

20.1.3. After a change adds, deletes, or replaces pages or affects page numbers. **NOTE:** A person other than the one making the change must do the page check.

20.1.4. Prior to destruction. This page check does not have to be recorded.

20.2. The COMSEC manager and CRO must ensure completed page checks of COMSEC publications. You do not need to check pages of PDO publications. COMSEC managers have the right to do or require additional page checks as needed. Unclassified documents do not require page checks unless page change value amendments are made to them.

20.3. Make page checks by:

20.3.1. Consulting the list of pages or the document cover.

20.3.2. Checking that each page is exactly as described.

20.3.3. Recording the check on the record of page checks page, or, if the publication has no record of page checks page, on the record of amendments page or front cover.

20.3.4. Annotate the date, signature, and command of the person making the check.

21. Amending Communications Security Publications. Take care not to lose individual pages when you amend COMSEC documents. In many cases, valid pages are inadvertently destroyed along with obsolete pages.

21.1. To eliminate carelessness, persons who make changes must follow these basic rules:

21.1.1. One person adds the new pages and also:

21.1.1.1. Checks the removed pages against the amendment instructions to make sure that only the obsolete pages were removed.

21.1.1.2. Records the change on the record of amendments page in the basic document.

21.1.2. A second person:

21.1.2.1. Checks the pages of the basic document against the current list of effective pages. Normally, you insert a new page in the basic document. Check the page number and the edition (i.e., original, amendment 1, amendment 2, etc.). A document can be numbered correctly even though it contains old pages that should have been replaced by new pages.

21.1.2.2. Records the change on the record of page checks page in the basic document.

21.2. Users amend publications they have received. COMSEC account personnel make amendments to publications held by the COMSEC account.

22. Accounting For and Disposing of Amendments.

22.1. Do not file handling instruction pages or write changes in the back of the basic document.

22.2. The COMSEC manager either directs you to destroy ALC-1 obsolete pages, complete a destruction certificate (SF 153) and send a copy to the COMSEC account, or return the obsolete pages to the COMSEC account for destruction.

22.3. The agency entering an ALC-4 amendment destroys the pages per paragraphs 25 through 28 after the second person checks pages.

23. Routine Destruction. To safeguard encrypted traffic and U.S. COMSEC operations, destroy superseded or obsolete COMSEC aids as soon as possible after the aids have served their purpose so it is impossible to reconstruct them. Superseded keying material is extremely sensitive because its compro-

mise potentially compromises all traffic encrypted with it as well. Be very careful not to accidentally destroy COMSEC aids.

24. Routine Destruction Security. Make facilities available for routinely destroying superseded keying material and other COMSEC material either within the facility or nearby so you can complete it without delay and without losing or compromising material being transported to the destruction facility. After destroying the material, check the destruction remains, the destruction equipment, and the surrounding area to make sure that destruction is complete and that you left no pieces behind.

25. Scheduling Routine Destruction.

25.1. Do not destroy COMSEC material before its supersession date unless you receive proper disposition instructions.

25.2. Destroy used keying material designated CRYPTO as soon as possible, but by 12 hours after supersession. Under special circumstances (e.g., destruction device not operational, etc.), local commanders or authorizing officials can grant an extension of up to 24 hours. **NOTE:** Offices using COMSEC material that do not normally operate during weekends (normal or extended) must destroy superseded material on the first duty day after the weekend.

25.2.1. Keep used or superseded keying material or extracts carried aboard special-purpose aircraft (e.g., airborne command posts, long-haul military flights, very important people transports) in secure storage until you reach secure destruction facilities; then destroy them as soon as possible. You do not need a waiver request under these circumstances.

25.2.2. Do not remove keytape segments stored in canisters until just before using or destroying them. Keep unused keytape segments in the keytape canister until the canister's effective period ends. If you take out any keytape segments, destroy all superseded keytape segments immediately. All other keytape segments in the keytape canister can stay there until needed or until the canister's effective period ends. Use AFCOMSEC Form 21, AFCOMSEC Form 22A, or AFCOMSEC Form 22B to record the individual keytape segments destroyed. **NOTES:** (1) If additional copies of the same key segment remain in the canister, destroy the used segment immediately after keying the equipment. Keep the last copy of the key segment until it is superseded and then destroy it within 12 hours after supersession. (2) If single-copy key is used, destroy key segments immediately after equipment rekeying if the circuit is very reliable. For unreliable circuits, single-copy segments may be kept for rekeying, but not longer than 12 hours after supersession. (3) Disposition records used for unclassified ALC-1 keying material are UNCLASSIFIED FOR OFFICIAL USE ONLY when filled in.

25.2.3. Keep pages, tables, and day sheets from codes and authenticators, if not removed, in the document until the document's effective period ends. If you remove any pages, immediately destroy all superseded pages. Record the destruction of individual pages, tables, day sheets, etc., from codes and authenticators on the destruction record page in the document (if provided), an SF 153, an AFCOMSEC Form 1, or an AFCOMSEC Form 11, **Disposition Record for Codes and Authenticators**.

25.3. Destroy irregularly superseded maintenance and test keying material when it is no longer serviceable.

25.4. Destroy superseded general COMSEC documents (i.e., AFKAGs, KAOs, KAMs, etc.) within 15 days.

25.5. Destroy the remains of amendments you have made to classified COMSEC publications within five days.

25.6. Destroy compromised material and associated disposition forms (e.g., AFCOMSEC Forms 21, 22A, or 22B) within 12 hours after you receive disposition instructions or upon receipt of case closure from NSA or AFCA.

25.7. Destroy pages from one-time pads as they are used and record the destruction on the destruction record page in the document (if provided), an SF 153, an AFCOMSEC Form 1, or an AFCOMSEC Form 11.

25.8. Destroy correspondence about superseded documents when it is no longer valuable.

26. Routine Destruction Methods. The authorized methods for routinely destroying paper COMSEC aids are burning, pulverizing or chopping, crosscut shredding, and pulping. Destroy non-paper COMSEC aids authorized for routine destruction by burning, chopping or pulverizing, or chemically altering them. Consult the COMSEC manager for a list of NSA-approved paper destruction devices.

26.1. Paper COMSEC Aids. The following applies to classified COMSEC keying material and media that hold, describe, or implement a classified cryptographic logic. Such media include full maintenance manuals, cryptographic descriptions, drawings or cryptographic logic, specifications of cryptographic logic, and cryptographic software. Use the same methods to destroy all other paper COMSEC aids.

26.1.1. When burning paper COMSEC aids, the fire must reduce all material to white ash. Be sure no burned pieces escape, inspect ashes and, if necessary, break up or reduce them to sludge.

26.1.2. When pulping, pulverizing, or chopping paper COMSEC aids, break the material into bits no larger than 5 millimeters. NOTE: Do not pulp paper-Mylar-paper keytape, high wet strength paper (map stock), and durable-medium paper substitute (e.g., TYVEX olefin, polyethylene fiber); burn, chop, or crosscut shred them.

26.1.3. Do not place keying material in burn bags for destruction along with other classified waste.

26.1.4. Destruction devices must be approved by NSA, through AFCA prior to using for destruction of COMSEC material.

26.2. Non-Paper COMSEC Aids. Destroy the material so that no one can reconstruct it by physical, chemical, electrical, optical, or other means. The authorized methods of routinely destroying non-paper COMSEC aids are burning, melting, chopping, pulverizing, and chemical alteration.

26.2.1. Consult the COMSEC manager for a list of NSA-approved non-paper destruction devices and methods, including methods for destroying microforms and magnetic or electrical storage or recording media containing crypto information.

26.3. Plastic Canisters. The goal of destroying empty plastic canisters is disfiguring their sides. The Kanister Krusher II (plans available from HQ AFCA/GCI) is recommended and safe. An alternative is crushing the sides with a hammer or blunt instrument. Take safety precautions to prevent injuries caused by the shattering canister.

26.4. COMSEC Equipment and Components. Routine destruction of COMSEC equipment and components below depot level is NOT authorized. Turn in equipment accountable within the SBSS in accordance with AFMAN 23-110. Turn in equipment accountable within CMCS to the COMSEC manager.

27. Witnesses. A destruction official must actually destroy COMSEC material. The destruction official and a witnessing official must sign destruction reports, subject to the following rules:

27.1. The destruction official is an appropriately cleared, responsible individual. **NOTE:** Since there is no formal grade requirement, CROs must ensure officials are trustworthy and knowledgeable.

27.2. The witnessing official must have a clearance consistent with the material being destroyed. In tactical, mobile, or emergency conditions, the destruction official may waive clearance requirement of the witnessing official and limit the witnessing official's examination to the front cover of the material.

27.3. The destruction official and the witnessing official must not sign destruction reports until destruction is complete and they have checked the destruction machine and area.

28. Destruction Records. COMSEC user agencies are accountable for issued COMSEC material until they return it to the COMSEC account or destroy it. Before listing complete editions of COMSEC aids on destruction certificates (SF 153), make sure all individual segments, pages, tables, etc., are actually destroyed.

28.1. Disposal of ALC-1 Material:

28.1.1. Use the destruction certification form provided to record destruction of each key setting. Destroy unused, excess key settings with the last key setting, page, table, or day sheet, etc., with the last key setting used or within 12 hours after supersession.

28.1.2. Provide a copy of all completed ALC-1 disposition or destruction records to the COMSEC account not later than the first duty day after material supersession.

28.1.3. Maintain the original completed disposition or destruction record on file for two years according to AFMAN 37-139.

28.1.3.1. (Added-AFSPC) **Consecutively number CRO destruction certificates through the calendar year (i.e. D-01-2001, D-02-2001, 20010001, 20010002, or any other consecutive numbering system). If using "user CM2", then the "user CM2" automatically generated transaction number is acceptable.**

28.1.4. For items issued to transient or deploying aircrews not returning to your location, file a copy of the signed, annotated receipt with destruction certificates and keep it for two years after the yearly cutoff. Returning aircrews must immediately give unused material and destruction records to their CRO.

28.2. Disposal of ALC-4 Material:

28.2.1. Do not return ALC-4 material to the COMSEC account for destruction.

28.2.2. When the COMSEC manager directs, destroy this material, record destruction of classified documents on a SF 153, and keep the destruction certificate for two years according to AFMAN 37-139.

28.2.3. No witness or documentation is required when destroying unclassified ALC-4 materials.

28.3. (Added-AFSPC) **Corrections to the Transaction Date, Report Date, or Block 9 are to be made with a single line through the error and initialed by both the destruction and witnessing Official. Other administrative corrections will be made with a single line initialed by the correcting official. Any correction made to the form must be explained by a Memo for Record (MFR).**

Section F—Control of Top Secret Keying Material

29. Introduction. Top Secret keying material is our nation’s most sensitive keying material because it protects the most sensitive national security information. Losing it to an adversary can endanger all the information the key protects. Single-person access to Top Secret keying material increases opportunities for unauthorized handling, use, production, dissemination, removal, and possession of the material. So, give Top Secret keying material special protection. The goal is to increase security for all Top Secret keying material, including codes and authenticators, and Top Secret key generating equipment.

30. Exceptions. This section does not apply to:

30.1. Sealed authentication system (SAS) and permissive action link (PAL) material.

30.2. Unopened NSA protectively packaged material that contains authenticators and NSA-produced keytape canisters with one or more key segments. **NOTE:** Protective technologies’ pamphlets, available from the COMSEC managers, describe NSA protectively packaged materials.

30.3. Keys generated locally for immediate use. This directive does apply to locally generated keys in physical or electronic form held for future use (see the OIs for equipment that can generate key and NAG-16).

30.4. COMSEC material used in tactical situations. TPI handling is not required in tactical situations although users must be enrolled in CAP. A tactical situation is defined as a unit deployed and operating under field conditions (e.g., a deployed combat communications package).

31. Two-Person Integrity of Top Secret Keying Material. TPI is a storage and handling system that prohibits individual access to certain COMSEC keying material. It requires the presence of at least two authorized persons who know TPI procedures and can detect incorrect or unauthorized security procedures for the task being performed. All user activities with Top Secret keying material must handle, store, issue, transport, and destroy it under TPI control. Each user of Top Secret keying material and Top Secret key generators develops and uses procedures and controls to make sure lone individuals do not have access to Top Secret keying material (e.g., hard copy, set on permuter trays, or contained in electronic fill devices, etc.) and Top Secret key generators (e.g., KG-83s, KT-83s, etc.).

31.1. TPI handling is not required in tactical situations, although users must be enrolled in CAP. A tactical situation is defined as a unit deployed and operating under field conditions (e.g., a deployed combat communications package).

32. Production. Users who produce Top Secret keying material do so under no-lone zone controls.

33. Transportation. Follow these procedures for moving Top Secret keying material:

33.1. Local transport of Top Secret keying material:

33.1.1. Locally transporting Top Secret keying material not sealed in NSA-approved protective packaging requires TPI controls. Both persons moving the material must meet the requirements of AFI 33-210 and must sign a receipt for the material when they pick it up.

33.1.2. Locally transporting Top Secret keying material in NSA-approved protective packaging does not require TPI controls. However, lone individuals moving the material must have proper clearance and have been granted cryptographic access according to AFI 33-210. When they deliver the material to the user's duty section, a second individual must inspect the package for tampering and record the inspection on the user's copy of the receipt from the COMSEC account.

33.2. Consult the COMSEC manager for procedures for moving Top Secret keying material by U.S. military or U.S. flag commercial aircraft.

34. Storing Material.

34.1. Store Top Secret keying material, not in NSA protective packaging, under TPI controls. A segment is considered out of NSA protective packaging when the entire algorithm is exposed. Use two different three-position, dial-type, combination locks that no one person can open. When using two combination locks, the COMSEC user must identify each security container (i.e., lock 1, lock 2, safe 1, safe 2) and name, in writing, each person with authorized access to each combination. Store material in a special access control container, within a security container, in a security container within a vault, in a security container equipped with an electronic lock using the dual access mode, or in a security container with two combination locks. Make sure at least one combination lock is built-in, as in a vault door or in a security container drawer. Each lock must have a separate SF 702, **Security Container Check Sheet**. **NOTE:** Mobile environments and some facilities manned around the clock may not always have security containers that meet the built-in lock requirement. In these environments, appropriate personnel who do not know the lock's combination can act as guards.

34.2. Non-GSA approved security containers modified with two hasps and two approved, three position, dial-type, combination padlocks are authorized for TPI. Limit use of this container type to secure facilities manned around the clock or vaults.

34.3. TPI storage procedures are not required for Top Secret key in tactical situations.

34.3.1. In these situations units unable to meet normal TPI storage requirements must either:

34.3.1.1. Store Top Secret keying material in a standard, approved field safe or similar container secured by a padlock meeting Federal Specification FF-P-110.

34.3.1.2. Or, if adequate storage facilities are not available, keep Top Secret keying material under personal custody.

34.3.2. Procedures in effect must require inspections of protective packaging according to applicable protective technologies pamphlets.

35. Use.

35.1. Set up security procedures to prevent a lone individual from tampering with, altering, copying, or destroying keying material. COMSEC No-Lone Zone (CNLZ) controls require the presence of two authorized persons in the common area where the material is located unlike TPI controls that require two authorized persons to directly handle and safeguard the keying material (e.g., by accessing storage containers, moving material, keying and rekeying operations, and destroying material). However,

TPI controls always apply to initial keying and rekeying operations. **NOTE:** For TPI, CNLZs are defined as rooms or areas immediately around equipment where hard-copy key or permuter plugs are installed. CNLZs are not subject to AFI 31-209, *The Air Force Resource Protection Program*.

35.2. Set up CNLZ at user locations whenever:

35.2.1. Permuter trays are set up with Top Secret key, whether installed in the equipment or not.

35.2.2. Cryptographic equipment contains Top Secret key in hard-copy form.

36. Recording Combinations. To provide ready access to secured material in emergencies, keep a central record of all lock combinations used to protect Top Secret keying material in a secure container approved for Top Secret storage. Record each lock combination separately and package it using the SF 700.

37. Two-Person Integrity Incidents. Besides COMSEC incidents identified in AFI 33-212, report any violation of TPI or CNLZ requirements, including situations in which an individual not under the CAP program accesses Top Secret keying material alone without a valid waiver. **NOTE:** Since FAA elements do not completely participate in the Air Force Cryptographic Access Program, they are exempt from certain CAP requirements.

38. Waivers. Top Secret keying material not in NSA-approved protective packaging and Top Secret key generators require TPI unless a waiver is granted by HQ AFCA/GCI. Revised operational procedures or work schedules, or other unit-level initiatives may make waivers unnecessary. A lone person must not access Top Secret keying material until all concerned individuals who will have access to the Top Secret keying material have entered into the CAP and an approved waiver has been granted. The COMSEC manager can help you obtain cryptographic access and submit waiver requests.

Section G—Emergency Action Plans

39. Introduction. Each activity using COMSEC material must understand that emergencies could expose its classified COMSEC material to loss or compromise. Planning can prevent or reduce loss or compromise and help facilities cope with two types of emergencies: accidental and hostile. This section discusses different types of emergencies, emergency plans, precautionary actions, destruction methods and procedures, destruction priorities, necessary reports, and minimum standards for emergency planning.

40. Emergency Protection Planning.

40.1. Activities that hold classified ALC-1 or ALC-2 material must develop and maintain a current EAP (see Attachment 5) to protect material during emergencies.

40.2. Structure operating routines for COMSEC facilities to reduce the number and complexity of actions required to protect COMSEC material if there is an emergency. EAPs consist of task cards only and must be coordinated with the wing COMSEC manager.

40.3. All locations must plan for fire, natural disasters (such as flood, tornado, and earthquake), and bomb threats. Locations outside the Continental United States (CONUS), except Alaska, Guam, Hawaii, Puerto Rico, and U.S. Virgin Islands, must also plan for hostile actions (such as enemy attack, mob action, or civil uprising).

40.4. Units in direct combat support (combat communications units, combat readiness units, or units and users that need to move or rotate to locations outside the CONUS) write and maintain a precautionary and total phase of emergency destruction plans only for deployment outside the CONUS. Do not write precautionary and emergency destruction plans for these units or users for their CONUS in-garrison operations.

40.5. For fire, natural disasters, and bomb threats, plan for keeping the material secure until order returns.

40.6. When planning for hostile actions, include a precautionary destruction phase and a destruction phase. Planning for hostile actions must focus on safely evacuating or securely destroying COMSEC material.

41. Emergency Action Plan. The term “emergency action plan” refers to actions planned for use during various scenarios (e.g., fire, evacuation, and destruction). The type and location of a facility merit primary consideration when developing each emergency plan scenario.

41.1. The person most familiar with the amount and significance of the COMSEC material on hand (normally the CRO) must prepare the plan.

41.2. If the plan calls for destroying COMSEC material, the CRO must make sure all destruction material and devices are readily available and work well.

41.3. The plan must be realistic to accomplish its goals. Keep the goals simple. Consider these factors:

41.3.1. Duties must be clear and concise.

41.3.2. Each person with access to COMSEC material must know of the plan and its location. Persons who have duties under the plan (whether by name, job title, or position) must receive detailed instructions from the CRO on how to carry out their duties if the plan is implemented. Make sure all personnel familiarize themselves with the plan and the various duties so necessary assignment changes may be made. Rotate duties so everyone knows each duty.

41.3.3. Conduct reviews and training exercises at least once every 6 months. High risk areas practice training exercises at least once every 3 months. This ensures that all persons can effectively carry out their emergency duties.

41.3.3. (AFSPC) Units will designate 2 months (i.e. January and July) to perform reviews and training, and annotate the dates in the local OI. Document completion of the training on a certification sheet, similar to the [Attachment 7 \(Added-AFSPC\) Sample](#). Retain this documentation from one command functional review to the next command functional review. Use of CAMS to document Emergency Action Plan (EAP) dry run participation is not authorized.

41.3.4. Keep the plan current. Revise the plan, if necessary, based on the training exercises.

41.4. Planners must consider three emergency options:

41.4.1. Securing the material.

41.4.2. Removing the material from the emergency scene.

41.4.3. Destroying the material.

41.4.4. The plan must clearly show which option or mix of options will be used. Direct disaster planning toward maintaining positive control of the material until order returns. Plans for hostile actions must focus on actions that safely evacuate or destroy COMSEC material.

41.5. Use the plan when the commander decides forces and facilities cannot adequately protect classified COMSEC material from loss or capture. The commander must give the senior person in the area the authority to put the plan in action if conditions prevent contact with the commander. **NOTE:** Consult the COMSEC manager for a list of approved destruction devices.

42. Basic Contents of Plans. All plans should include these basic elements:

42.1. Classify according to subject.

42.2. Assign specific responsibilities by duty assignment and with alternates, if possible.

42.3. Authorize the senior member present to carry out the plan.

42.4. Locate COMSEC material by storage containers.

42.5. Schedule dry runs.

42.6. Safeguard COMSEC material as much as possible and report the destruction of COMSEC material to the COMSEC manager.

42.7. Include names, addresses, and telephone numbers of all persons and organizations to contact in an emergency.

42.8. Make task cards identifying specific actions to be accomplished to carry out the plan's objective. Develop task cards for each scenario. Practice using EAPs in "dry runs" of the actions on the task cards.

42.8.1. (Added-AFSPC) **In areas where emergency actions are driven by checklists, (such as command posts, missile operations, or other 24 hour operations, etc.), EAPs may be put into checklist format instead of on task cards.**

42.9. Make coordination part of the plan. Coordinate plans with the COMSEC manager. Coordinate the emergency plan, in writing.

42.10. Review and revise the plan at least once every 3 years or when it changes significantly.

43. Planning for Fire, Natural Disasters, and Bomb Threats. Plans for disasters must include:

43.1. Fire reporting and initial fire fighting by assigned personnel. The fire plan must contain instructions and precautions when admitting firefighters (including non-U.S. citizens) to areas with classified COMSEC material. For example, do not hinder firefighters' performance of their official duties; however, identify them so they may take inadvertent exposure oaths later, if necessary.

43.2. Assigning on-the-scene responsibility for protecting classified COMSEC material.

43.3. Securing classified COMSEC material and COMSEC records (i.e., inventories and hand receipts). Keep the procedures a simple "stow and go." Do not carry records or material from the facility.

43.4. Evacuating the area.

43.5. Inspecting the area and security containers after the emergency for possible entry or tampering.

43.6. Inventorying classified COMSEC material after the emergency and reporting losses or unauthorized exposure to the COMSEC manager.

43.7. Personnel should avoid loss of life or personal injury during efforts to protect COMSEC material.

44. Planning for Hostile Actions. Plans for hostile emergencies must define the possible situations (e.g., a gradual ordered withdrawal from a hostile environment where you must destroy COMSEC discretely to avert hostility, or a hasty retreat from full-blown hostilities). Planning must include:

44.1. Assessing the threat of various types of hostile actions at the activity and the threat which potential emergencies pose to the classified COMSEC material.

44.2. Assessing the availability and adequacy of physical security protection capabilities (e.g., perimeter controls, guard forces, and physical defenses at facilities where classified COMSEC material is held).

44.3. Identifying facilities for emergency evacuation of classified COMSEC material. Prepare an emergency evacuation plan for each COMSEC facility if the base has an evacuation plan. This plan must provide for adequate secure storage of evacuated COMSEC material at the relocation site and protection during transit. Except under extraordinary conditions (e.g., an urgent need to restore secure communications after relocation), destroy rather than evacuate classified COMSEC keying material.

44.4. Identifying facilities and procedures for destroying classified COMSEC material in an emergency.

44.5. Destroying classified COMSEC material as a precaution, particularly maintenance manuals and keying material, not needed to continue operations during the emergency.

44.6. Establishing emergency communications procedures.

45. Precautionary Actions. Normally, user agencies must destroy only superseded material. The fewer actions needed in an emergency, the more likely success. The following advance practices simplify emergency actions:

45.1. Hold only the minimum amount of COMSEC aids.

45.2. Destroy all superseded material immediately.

45.3. Store material so you can readily remove or destroy it. **NOTE:** The commander, with the advice of the COMSEC manager, determines which COMSEC aids to destroy before the actual emergency. If you receive orders for precautionary destruction, advise the COMSEC account so they can ask for replacement material after the danger passes.

45.4. For precautionary destruction, follow the priorities in paragraph 46. However, keep the COMSEC aids necessary to maintain essential operations until you receive orders for emergency destruction. Retain:

45.4.1. All equipment.

45.4.2. All operational and maintenance documents for the systems held (e.g., AFKAGs, KAOs, KAMs, etc.).

45.4.3. A 60-day supply of COMSEC aids.

45.5. Make sure records show which material you destroyed as a precaution.

45.6. Order precautionary destruction, destruction, or evacuation of material, depending on the nature and circumstances of the threat to the material.

46. Emergency Destruction Priorities. Divide classified COMSEC material to destroy in an emergency into three categories. When there are enough people and facilities, assign different persons to destroy each category, using separate destruction facilities and following assigned priorities. Destroy COMSEC material using these destruction priorities:

46.1. Keying Material. The most sensitive keying material is that which was used to encrypt information, including the current key setting and future editions of SAS and PAL material. In enemy hands, all the information encrypted with the material is endangered. If you follow routine destruction procedures, you will have little or no superseded material to destroy in an emergency. When prioritizing keying material for destruction in each category, place Top Secret material ahead of Secret and Confidential, shared material ahead of point-to-point material, and keylists and keytapes ahead of one-time systems such as tapes and pads.

46.1.1. All superseded keying material and future editions of SAS and PAL material.

46.1.2. All current keying settings (this includes zeroizing cryptographic equipment and removing and destroying current keylists and keytapes).

46.1.3. All keylists, keytapes, codes, and authenticators scheduled to become effective within the next 30 days.

46.1.4. All remaining future keying material.

46.2. COMSEC Documents. This category includes cryptographic maintenance manuals, OIs, and general publications. These documents contain useful information on the types of cryptographic equipment in use, the level of technology, and the organization and conduct of COMSEC operations.

46.2.1. Sensitive pages of cryptographic equipment maintenance manuals.

46.2.2. Other classified documents.

46.2.3. Classified COMSEC files.

46.3. Cryptographic Equipment. In an emergency, first destroy critical elements of the cryptographic equipment, denying the enemy a useful piece of equipment. The operating document for each machine tells how to rapidly and effectively destroy specific cryptographic elements. Remove and destroy (time permitting):

46.3.1. Readily removable classified items, such as printed circuit boards and module boards in the order listed in the applicable OIs.

46.3.2. Other classified parts or components. You do not need to destroy unclassified chassis and elements.

47. Combined Priority List. The priority list in paragraph 46. applies when personnel and destruction facilities are adequate. When personnel and facilities are limited, combine the priorities and destroy COMSEC material in the following order:

47.1. Superseded keying material, currently effective keying material, and future editions of SAS and PAL material.

47.2. Keying material that becomes effective within the next 30 days in this order:

47.2.1. Top Secret.

47.2.2. Secret.

47.2.3. Confidential.

47.3. Sensitive pages of cryptographic equipment maintenance manuals. See the document's list of effective pages, the list of sensitive pages, or the table of contents.

47.4. Classified elements of cryptographic equipment, in the order their OIs list.

47.5. Other classified COMSEC documents.

47.6. Other classified COMSEC keying material including all remaining future keying material.

47.7. Classified COMSEC files.

48. Methods and Extent of Emergency Destruction. Use any approved method for routinely destroying classified COMSEC material to destroying material in an emergency. Also, several sodium nitrate and thermite-incendiary techniques unsuitable for routine destruction serve well in emergencies. Consult the COMSEC manager for a description of specific destruction devices and the precautions to follow when using these devices.

48.1. Classified Printed COMSEC Aids. Destroy classified keying material and other classified COMSEC publications so that no one can reconstruct them. Use any device or method approved for routine destruction (burning, chopping, pulverizing, shredding, or pulping). Consult the COMSEC manager for additional acceptable methods.

48.2. Classified Cryptographic Equipment. Destroy classified cryptographic equipment so it can never be used again. If time permits, destroy equipment so its cryptographic logic cannot be reconstructed, by removing and destroying classified parts, such as certain circuit boards (see Air Force Systems Security Memorandum [AFSSM] 4003, [C] *Emergency Destruction of Communications Security Equipment Elements [U]*). After you have destroyed these classified elements, you do not need to destroy the rest of the equipment. Approved and effective methods of destroying cryptographic equipment are:

48.2.1. A sodium nitrate fire.

48.2.2. Incendiary cryptographic equipment destroyers.

48.2.3. Incinerator, in some cases, for printed circuit boards. Break the boards after removing them from the incinerator.

48.2.4. If no other facilities are available, use hand tools such as acetylene torches, sledge hammers, and fire axes.

49. Emergency Destruction Tools. In the event of an emergency use any tool available to complete destruction tasks. The following are suggested destruction tools:

49.1. Hammer: 3-pound ball or cross peen.

- 49.2. Cold chisel: 5 3/4 inch long, 1/2-inch wide tip.
- 49.3. Stubby screwdriver: 1-inch blade, 7/32-inch wide tip.
- 49.4. Screwdriver: 1 1/2-inch blade, 5/32-inch wide tip, and 6-inch blade, 5/16-inch wide tip.
- 49.5. Phillips screwdriver: Numbered 0 and 2.
- 49.6. Wrench: 5/16 inch, box and open-end combination.
- 49.7. Pliers: 5-inch diagonal cutting and heavy duty, lineman.
- 49.8. Crowbar.
- 49.9. Fire ax or sledge hammer.

50. Identifying Sensitive Pages in Maintenance Manuals. Consult the COMSEC manager for detailed instructions on identifying sensitive pages of maintenance manuals for emergency destruction.

51. Emergency Destruction in Aircraft. An aircraft emergency leaves little time to destroy classified cryptographic material; however, try to keep the material from enemy hands. Work out emergency procedures based on such factors as type and amount of COMSEC material on hand, area of operation, aircraft type, and crew size. Paragraph 46. outlines destruction priorities.

- 51.1. When the aircraft is over water and capture or other emergency seems imminent, zeroize cryptographic equipment. Shred the keying material and other associated crypto material as completely as possible and scatter them.
- 51.2. If the aircraft is over land in a friendly area, keep the crypto material in the aircraft.
- 51.3. If the aircraft is in danger of landing or crashing in a hostile area, try to shred or rip paper material before scattering it over the widest area possible.
- 51.4. Do not carry unneeded COMSEC material aboard an aircraft. Bring only material necessary to the mission and length of the flight to minimize the quantity of material to destroy in an emergency.
- 51.5. Personnel should avoid loss of life or personal injury during efforts to protect COMSEC material.

52. Reporting Precautionary and Total Destruction. Accurate information about precautionary or total destruction is second in importance only to material destruction. Report the facts of the destruction directly to the COMSEC manager as soon as possible using the fastest medium available. Reports must clearly state what material you destroyed, method of destruction, and the extent of destruction of items not completely destroyed which may be assumed to be compromised.

Section H—Communications Security Incidents

53. Communications Security Incident Reporting. The importance of reporting all known or suspected COMSEC incidents immediately cannot be overemphasized. Before issuing material or equipment, the COMSEC manager and CRO must ensure users know they must immediately report known, suspected, or possible incidents of compromised COMSEC materials.

53.1. Each user agency must immediately report to the COMSEC account any occurrence that may jeopardize the security of COMSEC material or the secure electrical transmission of national security information. Equipment-unique security documents also list reportable incidents. Some specific actions you must report are:

53.1.1. Physical Incidents. Loss of control, theft, recovery by salvage, improper destruction, tampering, unauthorized viewing, access, copying, etc.

53.1.2. Personnel Incidents. Any capture, attempted recruitment, known or suspected control by a hostile intelligence entity, or unauthorized absence or defection of an individual who knows or has access to COMSEC information or material.

53.1.3. Cryptographic Incidents. Any equipment malfunction or operator error that threatens the security of a cryptographic machine, auto-manual, or manual cryptographic system, including unauthorized use of COMSEC keying material or equipment.

53.2. Anyone who knows of the loss, unauthorized disclosure, or other possible threat to COMSEC aids or equipment reports its details without delay to the nearest CRO or COMSEC manager.

53.2.1. The CRO advises the COMSEC manager who prepares and submits the initial incident report per AFI 33-212.

53.2.2. The violating unit's commander appoints a commissioned officer, senior noncommissioned officer, or civilian (GS-9 or above) to inquire about the circumstances surrounding the incident. On the basis of the inquiry, the commander determines whether to conduct a formal investigation and whether to notify Air Force Office of Special Investigations (AFOSI).

53.3. The CRO and users must thoroughly search for material considered missing. Advise the COMSEC manager immediately if someone finds the item and describe the circumstances of its recovery.

53.4. The inquiry or investigating official contacts the COMSEC manager for information and completes the inquiry or investigation report per AFI 31-401.

53.5. If transient personnel are involved in a possible violation, provide their names, ranks, grades, SSNs, citizenship, primary duty organizations, duty positions or military occupational specialties, security clearances, if known, and nationalities to the nearest COMSEC manager.

54. Reporting Procedures. Immediately report possibly endangered classified COMSEC aids to the CRO or COMSEC manager. Do not talk about the nature of the incident using unsecure means because the events surrounding a security incident may be classified.

Section I—Communications Security Inspection Program

55. Communications Security Functional Review Program. The COMSEC functional review program provides an effective management tool to make sure that COMSEC procedures are properly followed.

56. Communications Security Functional Reviews. The COMSEC manager must conduct a functional review of COMSEC user's facilities semiannually at scheduled times. Using the AFCOMSEC Form 19, or the inspector program checklist, COMSEC managers make sure that COMSEC material is properly received, controlled, handled, safeguarded, stored, and destroyed per current directives. In addition, the

COMSEC account's MAJCOM also checks these users during the periodic command COMSEC functional review of the COMSEC account.

56.1. The COMSEC account notifies all COMSEC users of the upcoming functional reviews.

56.2. Users positively identify all COMSEC functional review personnel by comparing the identification card (DD Form 2, **Armed Forces Identification Card [Active, Reserve, and Retired]**, or AF Form 354, **Civilian Identification Card**) with the functional review message notice, TDY orders, or records the COMSEC manager provides, and sign them in on the AF Form 1109 or FAA Form 1600-8 (for FAA accounts).

56.3. The COMSEC manager and command functional review personnel may also conduct functional reviews without notice.

57. Functional Review Checklist. The COMSEC manager checks those items listed on the AFCOMSEC Form 19 when conducting functional reviews on COMSEC facilities. MAJCOMs and wings may supplement this form.

57.1. (Added-AFSPC) Use AF Form 4160, Information Assurance Assessment and Assistance Program (IAAP) Criteria, to perform functional reviews on AFSPC COMSEC facilities.

58. Wing Communications Security Functional Review Procedures.

58.1. Functional review personnel prepare a narrative report identifying the user's rating, individual discrepancies and references, and recommend corrective actions.

58.2. Functional review personnel forward the report through the CRO's commander to the CRO for reply back to the COMSEC account.

58.3. The CRO reports on corrective actions taken or in progress, makes other comments, and forwards the report to the COMSEC manager, through the CRO's commander, by the deadline the COMSEC manager sets.

58.4. The CRO's commander must endorse the report.

58.5. Keep all functional review reports on file for review by command COMSEC functional review personnel.

58.6. If a user is rated "Unsatisfactory," the base COMSEC manager notifies the CRO's commander in person and conducts another functional review within 90 days.

59. Forms Prescribed. AFCOMSEC Forms 1 and 30 are prescribed by this AFI.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

Publications:

AFPD 33-2, *Information Protection*

AFMAN 23-110, *USAF Supply Manual*

AFI 31-209, *The Air Force Resource Protection Program*

AFI 31-401, *Managing the Information Security Program*

AFI 31-501, *Personnel Security Program Management*

AFI 33-210, *Cryptographic Access*

AFI 33-212, *Reporting COMSEC Incidents*

AFMAN 33-272, (S) *Classifying Communications Security and TEMPEST Information (U)*

AFMAN 37-139, *Records Disposition Schedule (will convert to AFMAN 33-339)*

AFIND 9, *Numerical Index of Departmental Forms*

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

AFSSI 3021, (FOUO) *Interim Operational Security Doctrine for the AN/CYZ-10/A Data Transfer Device (DTD) (U)*

AFSSM 4003, (C) *Emergency Destruction of Communications Security Equipment Elements (U)*

AFSSI 4100, (C) *Communications Security (COMSEC) Program (U)*

CJCSI 3260.1, (S) *Policy Governing JCS Material (U)*

Abbreviations and Acronyms

ACN—Accounting Control Number

AFCOMSEC—Air Force Communications Security

AFI—Air Force Instruction

AFIND—Air Force Index

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Memorandum

ALC—Accounting Legend Code

ASCAS—Automated Security Clearance Approval System

AFTO—Air Force Technical Order
CAP—Cryptographic Access Program
CCI—Controlled Cryptographic Item
CJCSI—Chairman of the Joint Chiefs of Staff Instruction
CMCS—COMSEC Material Control System
CNLZ—COMSEC No-Lone Zone
COMSEC—Communications Security
CONUS—Continental United States
COR—Central Office of Record
CRO—COMSEC Responsible Officer
DRU—Direct Reporting Unit
DTD—Data Transfer Device
EAP—Emergency Action Plan
EOM—End of Month
FAA—Federal Aviation Administration
FOA—Field Operating Agency
GS—General Schedule
GSA—General Services Administration
MAJCOM—Major Command
NATO—North Atlantic Treaty Organization
NSA—National Security Agency
OI—Operating Instruction
PAL—Permissive Action Link
PDO—Publications Distribution Office
PROM—Programmable Read-Only Memory
RON—Remain Overnight
SAS—Sealed Authentication System
SBSS—Standard Base Supply System
SF—Standard Form
SRO—STU Responsible Officer
SSN—Social Security Number
STU—Secure Telephone Unit

TO—Technical Order

TPI—Two-Person Integrity

U.S.—United States

Terms

Authorizing Official—The official who authorizes individuals to perform COMSEC responsibilities. At the wing level the staff directorate (two-letter personnel under the commander) is the authorizing official. At the group level and below the commander is the authorizing official.

COMSEC Aids—COMSEC material, other than equipment or devices, that helps to secure telecommunications and is needed to produce, operate, or maintain COMSEC systems and their components. Some examples are COMSEC keying material (items such as codes, keytapes, keylists, authenticators, one-time pads, etc., marked CRYPTO), callsign or frequency systems, and supporting documentation such as operating and maintenance manuals.

COMSEC Manager—Individual responsible for managing the COMSEC resources of a COMSEC account. Previously known as **COMSEC Custodian**.

COMSEC Material—An item that secures or authenticates telecommunications. (COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that holds or describes cryptographic logic, and other items for COMSEC functions.)

COMSEC Material Control System (CMCS)—The logistics system for distributing, controlling, and protecting COMSEC material. It consists of all COMSEC central offices of record, cryptological depots, and COMSEC accounts.

COMSEC Operations—COMSEC operations include distributing, safeguarding, destroying, and accounting for all COMSEC material at all administrative and operational COMSEC accounts and all COMSEC user locations.

COMSEC Responsible Officer (CRO)—The individual within an office or area responsible for COMSEC material received from the CMCS.

COMSEC Users—Individuals who have access to COMSEC material and must use and safeguard COMSEC material to perform their official duties.

Attachment 2

**SAMPLE APPOINTMENT LETTER FOR COMMUNICATIONS SECURITY
RESPONSIBLE OFFICERS AND ALTERNATES**

(Unit Letterhead)

MEMORANDUM FOR COMSEC ACCOUNT _____ *(Date)*

FROM: CC

SUBJECT: COMSEC Authorization Appointment Letter

1. The individuals listed below have been appointed the COMSEC Responsible Officer or alternate for COMSEC aids (identify unit and office symbol). Appointees can receive and carry all COMSEC aids issued, up to and including the classification indicated directly between _____ *(COMSEC account)*, Building ____ and _____ *(user location building number)*. They will make sure the aids they receive are entered on their daily inventory and are responsible for their safekeeping and for other actions required of users of COMSEC aids by AFI 33-211. These individuals have been granted access to classified COMSEC information and appropriate documentation is on file.

SSN/CivilianDutyAfter Hours

Rank/NameID NumberClearancePhonePhone

2. Please brief and train the newly appointed individuals per AFI 33-211, paragraph 4.1.6.
3. This letter supersedes all previous letters from this office on this subject (or give specific dates).

(Signature Element of Authorizing Official)

cc: Each individual

Attachment 3

SAMPLE COMMUNICATIONS SECURITY REQUIREMENTS LETTER

(Unit Letterhead)

MEMORANDUM FOR COMSEC ACCOUNT _____(Date)

FROM: *(Your unit office symbol)*

SUBJECT: COMSEC Requirements

1. COMSEC requirements for *(organization and office symbol)* are:

a. *(Enter the short title of documents and quantity needed.)*

b. *(If you request more copies of material you already have, give the number of copies you have and the new total you require.)*

c. *(Enter the date you need the material.)*

2. Authorization or Justification. *(If you ask for new COMSEC material, include copies describing the use of the actual authority or justification request or excerpts detailing the material's use. Justification for all requirements, including existing needs, must be specific; e.g., "HQ AFCA requires material in support of OPERATION PLAN [Oplan], JCS Exercise _____, etc." General statements, such as "to fulfill mission requirements" or "as directed by XYZ message 091234Z Jan 90," are not accepted by themselves; we need further justification.)*

(Signature Element of CRO)

Attachment 4

SAMPLE COMMUNICATIONS SECURITY ACCESS LIST

(Unit Letterhead)

MEMORANDUM FOR COMSEC ACCOUNT _____(Date)

FROM: *(Your unit office symbol)*

SUBJECT: COMSEC Access List

1. I grant these individuals access to this user's COMSEC material and have filed appropriate documentation for them. They have a valid need to know and the security clearance indicated.

RANK	NAME	SSN	CLEARANCE
-------------	-------------	------------	------------------

2. All personnel with an asterisk (*) next to their name have authority to grant access to others not listed who have a valid need to know. They will sign these individuals in on AF Form 1109, **Visitor Register Log**, before giving them access to COMSEC information.

3. This letter supersedes all previous letters from this office on this subject *(or give specific dates)*.

*(Signature Element of Commander,
Authorizing Official, or CRO)*

Attachment 5

SAMPLE--COMMUNICATIONS SECURITY EMERGENCY ACTION PLAN

Fire Task Cards

1. Task Card #1:

- a. Purpose. Provides for orderly evacuation of personnel and protection of COMSEC material within facilities using COMSEC aids and equipment in case of fire.
- b. The senior person present implements the plan by issuing task cards. If a limited number of personnel is available to carry out each task, combine the tasks.
- c. After the fire is out, inspect the safes for signs of entry or tampering and take a complete -inventory of all COMSEC material.
- d. If you find evidence of tampering or damage, thoroughly page check all COMSEC items.
- e. If items are damaged or missing, or if you suspect unauthorized exposure, notify the COMSEC manager immediately.

2. Task Card #2:

- a. Sound alarm and notify Fire Department, stating: THIS IS (*Rank/Name*), REPORTING A FIRE IN BUILDING _____, ROOM _____.
- b. Do not hang up the telephone until the fire dispatcher knows the location and has no questions.
- c. Report back to the senior person for further instructions.

3. Task Card #3:

- a. Secure all COMSEC material (keytapes, keylists, code books, KL-43, etc.), the STU-III keys, and all other classified material in the safe along with COMSEC inventories.
- b. Report back to the senior person for further instructions.

4. Task Card #4:

- a. Fight any open fire, if possible, using available fire extinguishers.
- b. Fire extinguisher(s) _____ (*Type*) _____ is/are located _____ (*Where*) _____.

5. Task Card #5:

- a. Open and guard the door that gives fire department personnel greatest access to the fire.
- b. Admit all firefighting personnel, including local national firefighters.

6. Task Card #6:

a. Notify the following personnel:

(1) Commander (*applicable unit*).

(2) CRO (*applicable unit*).

(3) Manager, COMSEC account _____ (duty hour phone number _____ and nonduty hour phone number _____).

b. Report back to the senior person for further instructions.

Natural Disaster Task Cards

1. Task Card #1.

a. Purpose. To protect COMSEC material in facilities using COMSEC aids and equipment in the event of a natural disaster (e.g., flood, earthquake, hurricane, etc.).

b. For natural disasters that require evacuation of the facility or seriously impair its physical security, the senior person implements this plan by issuing the remaining task cards. If a limited number of personnel is available to carry out the tasks, combine the tasks.

c. After the emergency, inspect the safes for signs of entry or tampering, and completely inventory of all COMSEC material.

d. If you find evidence of tampering or damage, thoroughly page check all COMSEC items.

e. If items are damaged or missing, or if you suspect unauthorized exposure, notify the COMSEC manager immediately.

2. Task Card #2:

a. Contact the following personnel:

(1) Commander (*applicable unit*).

(2) CRO (*applicable unit*).

3. Task Card #3: If time and circumstances permit, destroy all superseded COMSEC material and annotate the destruction.

4. Task Card #4:

a. Secure all other COMSEC material (e.g., keytapes, keylists, code books, KL-43, etc.), the STU-III keys, and classified material in the safe along with COMSEC inventories.

Bomb Threat Task Cards

1. Task Card #1:

- a. Purpose. To protect COMSEC material in facilities using COMSEC aids and equipment in the event of a bomb threat.
- b. In the event of a bomb threat, the senior person implements the plan by issuing the remaining task cards. If a limited number of personnel is available to carry out the tasks, combine the tasks.
- c. After the emergency, inspect the safes for signs of entry or tampering, and completely inventory all COMSEC material.
- d. If you find evidence of tampering or damage, thoroughly page check all COMSEC items.
- e. If items are damaged or missing, or you suspect unauthorized exposure, notify the COMSEC manager immediately.

2. Task Card #2: Contact the following personnel:

- a. Commander (applicable unit).
- b. CRO (applicable unit).

3. Task Card #3:

- a. Gather and secure all COMSEC material (keytapes, keylists, code books, KL-43, etc.), the STU-III keys, and classified material in the safe along with the COMSEC inventories.
- b. Leave the building and go to the designated assembly point.

4. Task Card #4:

- a. Conduct a search of the area and look for suspicious objects.
- b. If found, guard the entrance and admit only authorized personnel until security police take over.
- c. If not found, leave the building and go to the designated assembly point.

Emergency Evacuation Task Cards

1. Task Card #1:

- a. Purpose. To protect COMSEC material in facilities using COMSEC aids and equipment during emergency evacuation.
- b. For emergencies that require evacuation of a facility or seriously impair its physical security, the senior member present distributes the remaining task cards and oversees the evacuation. If a limited number of personnel is available to carry out the tasks, combine the tasks.
- c. After the emergency, completely inventory all COMSEC material.
- d. If you suspect tampering or damage, thoroughly page check all COMSEC items.

e. If items are damaged or missing, or if you suspect unauthorized exposure, notify the COMSEC manager immediately.

2. Task Card #2: Contact the following personnel:

- a. Commander (applicable unit).
- b. CRO (applicable unit).
- c. COMSEC manager.

3. Task Card #3:

- a. If time permits, destroy all superseded COMSEC aids.
- b. Report back to the senior person for further instructions.

4. Task Card #4:

- a. Gather all current material required for immediate secure communications, as well as the COMSEC inventory, and put them in a canvas bag.
- b. Report back to the senior person for further instructions.

5. Task Card #5:

- a. Remove COMSEC aids in use from all COMSEC equipment and put them in a canvas bag.
- b. Report back to the senior person for further instructions.

6. Task Card #6:

- a. Secure the facility as well as possible so forced entry will be obvious.
- b. Report back to the senior person for further instructions.

7. Task Card #7:

- a. If you expect to evacuate for a short time, secure all other COMSEC items (including future COMSEC aids) in an approved storage container.
- b. Put material required to maintain secure communications in a canvas bag.
- c. Report back to the senior person for further instructions.

8. Task Card #8: Evacuate the material, under constant surveillance, preferably by authorized personnel, to the designated evacuation site and begin secure communications.

Emergency Destruction Task Cards

Phase I--Precautionary Destruction Task Cards:

1. Task Card #1:

a. Purpose: To provide guidelines for:

(1) Destroying COMSEC material during emergencies resulting from natural, accidental, or hostile causes.

(2) Reducing holdings as a precautionary measure.

(3) Preventing their capture or compromise in an actual emergency or attack.

b. Personnel authorized to implement this plan:

(1) Commander (applicable unit).

(2) Commander (issuing COMSEC account unit).

(3) Manager, COMSEC account.

(4) CRO or alternate.

(5) Senior member present.

c. After completing precautionary destruction, record all destruction on the pre-addressed precautionary destruction letter and hand carry it to the COMSEC manager.

2. Task Card #2:

a. Contact the following personnel:

(1) Commander (applicable unit).

(2) CRO (applicable unit).

(3) COMSEC manager.

b. Report back to the senior person for further instructions.

3. Task Card #3:

a. Gather all COMSEC accounting records (i.e., inventories, destruction reports, hand receipts, etc.) and give them to the senior person present for safekeeping.

b. Gather the current month's inventory from the safe, take it to the incinerator room, and wait until someone brings material for you to destroy.

c. As you destroy each item, mark it off on the inventory form (AFCOMSEC Form 16).

d. Report back to the senior person for further instructions.

4. Task Card #4:

- a. Go to the incinerator in Building _____ and fire it up.
- b. The material for destruction is brought to you.
- c. Place it in the incinerator as you receive it.
- d. Tend the incinerator until all material is burned.
- e. Report back to the senior person for further instructions.

5. Task Card #5:

- a. Gather all superseded COMSEC aids, using the attached Priority of Destruction list, and place in canvas bags.
- b. Take the bags to the incinerator for destruction.
- c. Report back to the senior person for further instructions.

6. Task Card #6:

- a. Gather all future COMSEC aids (those not scheduled to go into effect within the next 60 days) COMSEC aids, using the destruction priority listing, and place in canvas bags.
- b. Take the bags to the incinerator for destruction.
- c. Report back to the senior person for further instructions.

7. Task Card #7:

- a. Gather all administrative documents, files, training aids, and other material not required for continued operations and place in canvas bags.
- b. Take the bags to the incinerator for destruction.
- c. Report back to the senior person for further instructions.

Phase II--Total Emergency Destruction Task Cards:

1. Task Card #1:

- a. Purpose: To provide guidance for preventing capture or compromise of COMSEC material in an actual emergency or attack.
- b. The commander of the applicable unit, the commander of the issuing COMSEC account, the COMSEC manager account number _____, the CRO or alternate, or the senior member present may implement this plan. They do this by distributing the remaining task cards and monitoring task completion.

c. After emergency destruction or as soon as possible if emergency destruction is not completed, record all destruction on the pre-addressed emergency destruction letter (*see Attachment 6*) and carry it to the COMSEC manager.

2. Task Card #2:

a. Notify the following personnel:

(1) Commander (applicable unit).

(2) CRO (applicable unit).

(3) COMSEC manager.

b. Report back to the senior person for further instructions.

3. Task Card #3:

a. Gather the current month's inventory from the safe, take it to the incinerator room, and wait until someone brings you material for destruction.

b. As you destroy each item, check it off on the inventory form (AFCOMSEC Form 16).

c. Report back to the senior person for further instructions.

4. Task Card #4:

a. Go to the incinerator in Building ____ and fire it up. Wait there until someone brings you material for destruction.

b. Place the material in the incinerator when you receive it.

c. Tend the incinerator until all the material is burned.

d. Report back to me for further instructions.

e. Report back to the senior person for further instructions.

5. Task Card #5:

a. Declassify all COMSEC equipment by removing the key and zeroizing.

b. Gather all COMSEC aids using the destruction priority list and place it in canvas bags.

c. Take the bags to the incinerator for destruction.

d. Report back to the senior person for further instructions.

6. Task Card #6:

a. Gather all current COMSEC aids, using the priority of destruction list, and place them in canvas bags.

b. Take the bags to the incinerator for destruction.

c. Report back to the senior person for further instructions.

7. Task Card #7:

- a. Remove all classified and CCI boards from the COMSEC equipment, thoroughly smash them with a hammer or an ax, and scatter the pieces.
- b. Document destruction on the COMSEC inventory (AFCOMSEC Form 16).
- c. Write names of unlisted items on the back of the form.
- d. Report back to the senior person for further instructions.

PRIORITY OF DESTRUCTION

(Include, as a minimum, the following elements in your priority of destruction documentation: priority, locations, short titles of material, and safe number)

Keying Material

- 1. All superseded keying material and future editions of sealed authentication system (SAS) and permissive action list (PAL) material:
 - a. Top Secret (shared material ahead of point-to-point).
 - b. Secret (shared material ahead of point-to-point).
 - c. Confidential (shared information ahead of point-to-point).

- 2. All current keying material (zeroize all cryptographic equipment and remove and destroy current keylists and keytapes).
 - a. Top Secret (shared information ahead of point-to-point).
 - b. Secret (shared information ahead of point-to-point).
 - c. Confidential (shared information ahead of point-to-point).

- 3. All future keylists, keytapes, codes, and authenticators scheduled to take effect within the next 30 days:
 - a. Top Secret (shared information).
 - b. Secret (shared information).
 - c. Confidential (shared information).

- 4. All remaining future keying material.

COMSEC Documents

1. Sensitive pages of cryptographic equipment maintenance manuals.
2. Remaining classified documents.
3. Classified COMSEC files.

Cryptographic Equipment

Remove and destroy (time permitting), and list location.

- a. Readily removable classified and sensitive (CCI) elements.
- b. Remaining classified and sensitive (CCI) parts or components.

Attachment 6

SAMPLE--PRECAUTIONARY OR EMERGENCY DESTRUCTION LETTER

MEMORANDUM FOR (COMSEC Account Number)

FROM: (Unit Office Symbol)

SUBJECT: Precautionary Destruction or Total Emergency Destruction

We destroyed the following items according to the (unit identification) Emergency Action Plan (include: Short title and edition, quantity, publication number, method [shred, burn, or smash], and percent destroyed).

(Signature of Destroying Official)(Signature of Witnessing Official)
(Typed Name, Rank, Branch of Service)(Typed Name, Rank, Branch of Service)

(Date of Destruction)

Attachment 7 (Added-AFSPC)

SAMPLE CERTIFICATION SHEET

1. The following individuals certify that they are familiar with and have performed a dry run of all COMSEC emergency action plans:

SECTION: _____ MONTH _____ YEAR _____

(Unit/Office Symbol)

NAME SIGNATURE DATE RESULTS

2. Remarks (Continue on reverse if necessary):

3. The following people were not able to attend and will be rescheduled at a later time.

4. I certify that I have conducted dry-run training for all personnel listed above on the date indicated.

Signature of person conducting training

(Date)

Attachment 8 (Added-AFSPC)

ELECTRONIC DISPOSITION RECORD

Table A8.1. Electronic/Generated Key Management Log (CONFIDENTIAL WHEN FILLED IN)

Note: Signing constitutes an understanding of the proper protection, inventory, storage, destruction and usage procedures.

DATA TRANSFER DEVICE:												
SHORT TITLE	ED	CLASS	EFF DATE	SUP DATE	ACTION			CIRCUIT/ EQUIP	REMARKS	DATE	SIGNATURES	
					UPLD	DNLD	OTHER				ACTION OFFICIAL	WITNESS