BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-211

3 JUNE 2004

Communications and Information

COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFCA/WFP
(Mr. James N. Plummer, Jr.)
Supersedes AFI 33-211, 31 OCTOBER 2003

Certified by: HQ USAF/XICI
(Col Linda K. McMahon)
Pages: 88
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*); AFI 33-201, *Communications Security (COMSEC)(FOUO)*; 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 issues to them. This instruction applies to all Air Force military, civilian, and contractor personnel under contract by the Department of Defense (DoD) who handle COMSEC materials. This instruction takes precedence over all conflicting Air Force documents. Additional instructions and manuals are listed on the Air Force Publishing Web site at Uniform Resource Locator (URL): **http://www.e-publishing.af.mil** under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/WFP, and Headquarters United States Air Force (HQ USAF/XICI), 1800 Air Force Pentagon, Washington DC 20330-1800. Major commands (MAJCOM), field operating agencies (FOA), and direct reporting units (DRU) send one copy of final supplement to HQ AFCA/WFP and HQ AFCA/ITXD. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force Web-RIMS *Records Disposition Schedule (RDS)* located at **https://webrims.amc.af.mil/rds/index.cfm**. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*, affect this publication. See **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2004-1. The update provides references to specific instructions for the handling of NATO, NATO Nuclear Command and Control COMSEC materials, and positive control materials. The change requires the COMSEC manager to coordinate on all requests for new COMSEC equipment. It requires training for all personnel on the access lists and deletes the CRO and alternate CRO from training. This change adds procedures to establish material distribution if unit is deployed more than 6 months. This update deletes the usage of AFCOMSEC Forms 21, 22A, and 22B and establishes use of the disposition record cards only. The update changes the CIK of a DTD that holds SCI keying material to be stored in under TPI controls. This update provides additional information about the software program, Users Computerized Management of COMSEC Material (UCM^2). This change deletes the requirement to use "red ink" and "green ink" to "a specific color" on changes made to inventories. It adds instructions on who can sign appointment letters for contractors, and allows them to use a company form for visitor entry instead of an AF Form 1109. This update adds that the COMSEC manager provides the CRO with after duty hours notification contact numbers. It also adds that the COMSEC operational and maintenance manuals will be maintained for the equipment held by the user. The change adds instructions that the destruction and witnessing officials be physically present and that they never sign the destruction form in advance when destroying material.

Section A General Instructions 6

1. Introduction. 6
2. Objective. 6

Section B Management and Responsibilities for Communications Security Material 6

3. Communications Security Responsibilities. 6
4. Appointing COMSEC Responsible Officers (CRO). 9
5. Training. 9
6. Operating Instructions (OI). 10

Section C Administrative Security Procedures 10

7. Producing Communications Security Aids. 10
8. Communications Security Forms. 10
9. Records Maintenance and Disposition. 11
10. Standard Accounting Legend Codes (ALC). 11
11. Status Information. 12
12. Disposition Record Cards. 12

Section D Requesting, Issuing and Using COMSEC Materials 12

13. Requesting Communications Security Material. 12
14. Over-The-Counter Service. 13

15. Authorizing the Receipt and Transport of COMSEC Materials. 13
16. Issuing to Communications Security Users. 14
Section E Physical Security Requirements for Communications Security Operations 16
17. Physical Security Requirements. 16
18. Access Controls and Procedures. 16
19. Storing Communications Security Information and Material. 17
20. Security Checks. 20
Section F Safeguarding and Controlling 20
21. Inventory and Accounting Requirements. 20
22. Page Checks of Classified Communications Security Publications. 23
23. Amending Communications Security Publications. 23
24. Accounting For and Disposing of Amendments. 24
25. Photography. 24
26. Public Display of COMSEC Material. 24
Section G Destruction 24
27. Routine Destruction. 24
28. Routine Destruction Security. 25
29. Scheduling Routine Destruction. 25
30. Routine Destruction Methods. 27
31. Witnesses. 28
32. Destruction Records. 28
Section H Control of TOP SECRET Keying Material 29
33. Introduction. 29
34. Exceptions. 29
35. Two-Person Integrity (TPI) of TOP SECRET Keying Material. 29
36. Transportation. 29
37. Storing Material. 30
38. Use. 30
39. Recording Combinations. 31
40. Two-Person Integrity (TPI) Incidents. 31
41. Waivers. 31

Section I Emergency Action Plans 31

42. Introduction. 31
43. Emergency Protection Planning. 31
44. Emergency Action Plan. 32
45. Basic Contents of Plans. 33
46. Planning for Fire, Natural Disasters, and Bomb Threats. 33
47. Planning for Hostile Actions. 34
48. Precautionary Actions. 34
49. Emergency Destruction Priorities. 35
50. Combined Priority List. 36
51. Methods and Extent of Emergency Destruction. 36
52. Emergency Destruction Tools. 37
53. Identifying Sensitive Pages in Maintenance Manuals. 37
54. Emergency Destruction in Aircraft. 37
55. Reporting Precautionary and Total Destruction. 37

Section J Communications Security Deviations 38

56. Communications Security Deviations Reporting. 38
57. Reporting Procedures. 38

Section K Information Assurance Assessment and Assistance Program (IAAP) 39

58. Communications Security Assessment and Assistance Program. 39
59. Communications Security Assessment and Assistance. 39
60. Information Assurance Assessment and Assistance Program 39
61. Wing Communications Security Assessment/Audit Procedures. 39
62. Information Collections, Records, and Forms. 40

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 41

Attachment 2—SAMPLE APPOINTMENT LETTER FOR COMMUNICATIONS SECURITYRESPONSIBLE OFFICERS AND ALTERNATES 45

Attachment 3—SAMPLE COMMUNICATIONS SECURITY REQUIREMENTS LETTER 46

Attachment 4—SAMPLE COMMUNICATIONS SECURITY ACCESS LIST 47

Attachment 5—SAMPLE -- COMMUNICATIONS SECURITY EMERGENCY ACTION PLAN 48

Attachment 6—SAMPLE -- PRECAUTIONARY OR EMERGENCY DESTRUCTION LETTER 57

Attachment 7—HANDLING INSTRUCTIONS FOR ALL KEYTAPES 58

Attachment 8—IC 2003-1 TO AIR FORCE INSTRUCTION 33-211, COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS 60

Attachment 9—IC 2004-1 TO AIR FORCE INSTRUCTION 33-211, COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS 78

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 materials.

1.1. Safeguard and control NATO Nuclear Command and Control COMSEC Material as described in AMSG-773, *Policy and Procedures for Handling and Control of Two-Person Controlled (TPC) NATO Sealed Authentication System (SAS).*

1.2. Safeguard and control other NATO material as prescribed in AMSG-293, *NATO Cryptographic Instruction*.

1.3. Safeguard and control Joint Staff positive control material and devices (i.e., Sealed Authenticator System, Permissive Action Link, Coded Switch System, Positive Enable System, and Nuclear Certified Computer Data) as prescribed in Chairman Joint Chiefs of Staff Instruction (CJCSI) 3260.01, *Policy Governing Positive Control Material*.

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. Communications Security Responsibilities.

3.1. COMSEC Manager. Specific duties and responsibilities for the COMSEC manager are defined in AFKAG-1, *Air Force Communications Security (COMSEC) Operations*. The local COMSEC manager:

3.1.1. Receives all COMSEC materials intended for issue to CROs, issues all COMSEC material on Standard Form (SF) 153, **COMSEC Material Report**, and instructs CROs and alternates, in writing, on use, control, and storage of the COMSEC materials.

3.1.2. Audits and inventories user's accounting legend codes (ALC)-1 and ALC-2 COMSEC material control system (CMCS); ALC-6 and ALC-7 Electronic Key Management System (EKMS) holdings.

3.1.3. Provides guidance on setting up CRO functions.

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

3.1.5. Provides the required status information before issuing COMSEC aids.

3.1.6. Trains CRO and alternate CROs.

3.1.7. Ensures another CRO signs for COMSEC materials when a CRO transfers or cryptographic access is suspended .

3.1.8. Ensures CROs have the applicable operating instructions (e.g., AFKAO, KAO) and system security instructions (e.g., Air Force Systems Security Instructions [AFSSI]) for all COMSEC equipment held.

3.1.9. Perform semiannual assessments and audits of the CRO according to AFI 33-230, Information Protection Assessment and Assistance Program (to become Information Assurance Assessment and Assistance Program) and AFKAG 2, Air Force COMSEC Accounting Manual.

3.1.10. Coordinate on AF Form 3215, **C4 Systems Requirement Document**, identifying COMSEC equipment requirements, and order COMSEC devices that are in COMSEC Material Control System (CMCS) according to AFKAG 2.

3.1.11. Provide a contact number for non-duty notification to the CRO and users to report all known or suspected COMSEC deviations.

3.2. Commander. The commander of each unit that needs COMSEC materials:

3.2.1. Ensures a CRO and at least one alternate is appointed in writing to receive COMSEC materials.

3.2.2. Ensures that adequate, approved security containers or facilities are available for storing COMSEC materials.

3.2.3. Takes immediate, corrective action in response to discrepancies identified during command COMSEC assessments or wing COMSEC manager semiannual assessments. All assessment reports require the commander's review for action and endorsement.

3.2.4. May appoint more than one CRO in large units, depending on the number of COMSEC users and the volume of material handled. Appoints CROs according to paragraph **4.**

3.2.5. Ensures that a National Security Agency (NSA)-approved destruction device is readily available.

3.2.6. Takes required action involving COMSEC deviations according to **Section J** and AFI 33-212, *Reporting COMSEC Deviations*.

3.3. CROs:

3.3.1. Notify the COMSEC Manager, in writing, of any new requirements, changes (increase or decrease), or pending requirements to existing requirements (See **Attachment 3**).

3.3.2. Review annually the requirement for COMSEC material according to paragraph **13.**

3.3.3. Make sure all persons granted access to COMSEC materials have a final security clearance equal to or greater than the classification level of the COMSEC material to be accessed and have a valid need-to-know.

3.3.4. Keep an accurate list of persons with authorized access to COMSEC holdings according to paragraph **18.** and see **Attachment 4**.

3.3.5. Conduct initial and refresher training of all COMSEC users according to paragraph **5.**

3.3.6. Take responsibility for receiving, accounting for, checking pages of, handling, using, and safeguarding all COMSEC material that they or their alternate receives until it is destroyed or returned to the COMSEC account. Maintain an exact copy of the hand receipt maintained at the COMSEC account for all material received.

3.3.7. Develop a local operating instructions (OI) according to paragraph **6.**

3.3.8. Perform inventories, according to paragraph **21.**

3.3.9. Verify COMSEC materials are inventoried according to their respective ALCs.

3.3.10. Carry out duties as deemed necessary by the COMSEC manager.

3.3.11. Issue COMSEC materials to user activities according to this instruction, when applicable.

3.3.12. Issue a receipt to in-transit personnel who turn in material for safekeeping. When the material is reclaimed retrieve the receipt for the material from the individual. Your accountability for the material ends .

3.3.13. Return or destroy all material as the COMSEC manager directs. Destroy COMSEC aids per **Section G**.

3.3.14. Keep all records according to AFMAN 37-139.

3.3.15. Develop an emergency action plan (EAP) that consists of task cards, coordinate it with the COMSEC manager for review and endorsement. Conduct EAP training according to **Section I**.

3.3.16. Ensure required security checks are performed according to paragraph **20.**

3.3.17. Provide an update report every 30 days on findings identified during assessments/audits, or as the COMSEC manager directs, until they are corrected.

3.3.18. Report all known or suspected COMSEC deviations to the COMSEC manager.

3.3.19. All personnel granted access to COMSEC must be familiar with applicable Air Force and specialized COMSEC publications (e.g., OIs, AFI 33-211, AFSSIs, KAMs, KAOs, etc.). These personnel must maintain this familiarization by accomplishing semiannual training. To validate this training all personnel will sign and date the review documentation developed by the CRO. Personnel on leave or temporary duty (TDY) must complete this training upon return to duty section.

3.3.20. Enroll all applicable personnel in the Cryptographic Access Program (CAP) as outlined in AFI 33-210, *Cryptographic Access Program,* and remove them from the CAP when they are removed from the access list.

3.3.21. Obtain relief of accountability from the COMSEC manager prior to leaving their current duty assignment. Ensure all COMSEC material is returned to the COMSEC manager and signed over to the new CRO.

3.3.22. Obtain new COMSEC equipment according to AFI 33-103, *Requirements Development and Processing*. Coordinate with the COMSEC manager on all requirements.

3.4. COMSEC Users. COMSEC users have access to COMSEC material and also the responsibility for safeguarding them. COMSEC's ultimate success or failure rests with the material's individual user. The careless user or the user who fails to follows procedures for using, safeguarding, and destroying COMSEC material wastes all security efforts. COMSEC users must ensure that anyone who receives COMSEC material has authorization and has verified the individual’s security clearance. Users must follow all security rules at all times. Report to the CRO or the COMSEC manager any circumstances, intentional or inadvertent acts, which could lead to the unauthorized disclosure of classified informa-

tion, including its loss, improper use, unauthorized viewing, or any other instance that could possibly jeopardize the value of COMSEC material. COMSEC users:

3.4.1. Safeguard COMSEC material according to this instruction and control the material locally until destroyed or turned in.

3.4.2. Return material to the CRO on request.

3.4.3. Maintain and familiarize themselves with correct procedures for operating associated cryptographic equipment and devices utilizing applicable AFSSIs, AFKAOs, KAOs, or instructions provided by the CRO.

3.4.4. Report immediately any known or suspected compromise of COMSEC material to the CRO or COMSEC manager according to AFI 33-212 and **Section J**.

3.4.5. Be trained by the CRO prior to being granted unescorted access to COMSEC materials according to paragraph **5.**

3.4.6. Obtain relief of accountability from the CRO prior to being relieved of duties as a COMSEC user. The CRO must ensure users are not signed for any COMSEC material.

4. Appointing COMSEC Responsible Officers (CRO). Unit commanders (or equivalents, Facility Security Officer for contractors) appoint, 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 materials to and from. Update this letter at least annually or as changes occur.

4.1. The person appointed as primary CRO must have a minimum grade of staff sergeant (E-5) or General Schedule (GS)-5. Alternates must have a minimum grade of senior airman (E-4) or GS-4.

4.1.1. 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.

4.1.2. 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 (US) personnel.

4.1.3. Appoint contractors as CROs, provided the requirement has been annotated on the Department of Defense (DD) Form 254, **DoD Contract Security Classification Specification,** or by a letter from the contracting monitor stating that the contractor has a requirement for COMSEC material. They must hold comparable grades required of government personnel .

4.2. Commanders approve waivers for personnel with lower grades. Process waivers through the COMSEC manager.

4.3. Change CROs if the CRO will be deployed or on TDY for more than 90 days, or is pending a transfer .

5. Training. CROs use this AFI and other applicable publications to set up a comprehensive, periodic training program for COMSEC Users. Training is mandatory for all personnel listed on the access list. Ensure all personnel with authorized access know how to handle, control, and use the COMSEC material. Ensure that all personnel are familiar with correct procedures in operating associated cryptographic

equipment utilizing applicable AFKAOs, KAOs, AFSSIs, or similar instruction provided by the COMSEC manager. Use AF Form 4168, **COMSEC Responsible Officer and User Training Checklist,** to document initial and refresher training of all users. Complete a separate training checklist for each person with access. Each block beside each item that applies must contain the initials of the trainer and trainee. Provide annual refresher training to all personnel who have been granted access. Accomplish training at least every 365 days. Document annual training by completing a new AF Form 4168. Maintain only the most current form on file.

6. Operating Instructions (OI). Each CRO must write COMSEC OIs and coordinate them with the COMSEC manager for review and endorsement prior to its implementation. The OIs contain provisions for securely conducting COMSEC operations (in both normal and emergency situations) and for safeguarding COMSEC material. The procedures and instructions in the OIs are specific to the user's activity. A contractor CRO may title its operating instructions as Standard Practice Procedure or by another other corporate nomenclature as long as it meets the requirements set by this instruction.

6.1. OIs should include procedures for cryptographic operations (e.g., how to use the COMSEC equipment), keytape verification, disposition procedures, local accountability for COMSEC material on handling, controlling, and protecting COMSEC assets, including inventory, TPI (if applicable), CAP (if applicable), COMSEC maintenance support (e.g., who to notify if the COMSEC equipment goes down), access restriction, storage, routine and emergency destruction, COMSEC deviation reporting, and a requirement for CROs to get the COMSEC manager's relief of accountability before leaving their current assignment.

6.2. COMSEC users must obtain relief of accountability through their CRO.

6.3. Units with a deployable mission will develop procedures on handling, controlling, and protecting COMSEC materials while deployed. Ensure these procedures are established in a separate OI for use when deployed, and it is marked or annotated to indicate clearly it is to be used only when on deployment. Maintain it separately from the in-garrison OI to avoid potential confusion.

Section C—Administrative Security Procedures

7. Producing Communications Security Aids. Only NSA, the Service cryptology elements, and EKMS elements (i.e., Local Management Device/Key Processor) are authorized to produce nomenclature and non-nomenclature COMSEC aids. Other Air Force activities must not originate, formulate, or produce keylists, codes, ciphers, call signs, authenticators, or any other form of COMSEC aids. Do not remove, copy, or reproduce any part of COMSEC keying material unless the controlling authority permits it or it is authorized in the COMSEC materials handling instructions. Other activities may make extracts from general publications when authorized in the document's handling instructions.

8. Communications Security Forms. Paragraph **62.3.** lists forms that are used to satisfy COMSEC needs. Forms are available on the Air Force publication worldwide web site (www) at **http://www.e-publishing.af.mil** or from the COMSEC manager. Most user forms are available in Users Computerized Management of COMSEC Material (UCM^2). Use of computer-generated forms is acceptable .

9. Records Maintenance and Disposition.

9.1. 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.

9.2. 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 .

9.2.1. Limit access to these records and files to those persons who manage, administer, operate, and maintain COMSEC aids and equipment. MAJCOM approval is required if outside agencies such as the Air Force Audit Agency or Inspector General require viewing of COMSEC documentation.

9.2.2. During record maintenance and administrative staff assistance visits and program management reviews, reviewers may only check the Records Information Management System (RIMS), Files Maintenance and Disposition Plan. Do not grant reviewers access to COMSEC materials, records, or files.

9.3. Do not use correction fluid or correction tape on COMSEC records that affect control and accountability of material. This includes SF 153; Air Force Communications Security (AFCOMSEC) Form 16, **COMSEC Account Daily-Shift Inventory;** disposition record cards (DRC); SF 700; **Security Container Information**; SF 701, **Activity Security Checklist**; and SF 702, **Security Container Check Sheet**. Use only original forms .

9.4. At a minimum the COMSEC records maintained by the CRO are operating instructions, emergency action plans, appointment letters, access list, requirements letter, AFCOMSEC Form 9, **Cryptographic Access Certificate (PA)**; AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**; AF Form 1109; **Visitor Register Log**; AFCOMSEC Form 16; AF Form 4168; DRC, destruction reports, hand receipts, waivers, EAP training, required reading, and semiannual assessments.

9.5. User Computerized Management of COMSEC Material (UCM^2) is the Air Force software program used to manage COMSEC material at the User account level. It consists of a computer database designed to assist COMSEC CROs in their daily accounting activity. UCM^2 facilitates the tedious day-to-day accounting, decreases accounting discrepancies, and reduces the required paperwork that audits COMSEC accounting transactions. UCM^2 must be loaded onto a standalone computer. UCM^2 becomes classified SECRET if the effective dates of COMSEC materials are entered. Do **NOT** enter UCM^2 onto the Secret Internet Protocol Router Network (SIPRNET).

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

10.1. ALC-1 material is continuously accountable by accounting number within the COMSEC 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 a General Services Administration (GSA) approved, locked security container.

10.1.1. Use AFCOMSEC Form 16 to make a inventory by short title, edition, accounting control number (ACN), and quantity, per paragraph **21.** .

10.1.2. Return material when the COMSEC manager asks for it. Destroy it upon supersession, only in an emergency, or as the COMSEC manager directs. In-transit aircrews will follow the instructions provided when they were issued the material (see paragraph **16.2.4.**) .

10.1.3. Request from the COMSEC manager in writing additional copies of the material according to paragraph **13.**

10.1.4. Safeguard and account for ALC-1 controlled cryptographic item (CCI) equipment when you receive it from the CMCS (e.g., AN/CYZ-10, etc.) on the AFCOMSEC Form 16. Semiannually inventory unclassified CCI equipment according to AFI 33-275, *Controlled Cryptographic Items*. Conduct inventories on CCI equipment received from the Standard Base Supply System (SBSS) (e.g., KG-84, STU-III, etc.) according to AFMAN 23-110, *USAF Supply Manual.*

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

10.3. Unless directed by the 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. Protect classified ALC-4 material 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.

10.4. ALC-6 is electronically generated key that is continuously accountable to the Central Office of Record (COR) by means of EKMS elements. Tier 0 or Tier 1 within the EKMS system generates the electronic key. Account for keys on hand receipts and local DRCs.

10.5. ALC-7 is electronically generated keying material that is continuously accountable locally within EKMS elements. Keys are generated locally by the COMSEC account. Account for keys on hand receipts and local disposition records (e.g., DRC, MAJCOM approved form, etc.).

11. Status Information. A COMSEC key's short title, alphabetical edition designator with its effective date of classified COMSEC keying material, is classified according to AFMAN 33-272 (S), *Classifying COMSEC and TEMPEST Information (U)* (will become Classifying Information Assurance Information). Never reveal it in unclassified correspondence. Report violations through the unit security manager as an information security incident according to AFI 31-401, *Information Security Program Management*. Effective dates of unclassified (including unclas crypto) keying material is considered unclassified.

12. Disposition Record Cards. The COMSEC manager enters the required status information on the Disposition Record Cards (created by the CRO using UCM[2]) or on the front covers before issuing COMSEC aids. When material is issued, date and initial each block individually.

Section D—Requesting, Issuing and Using COMSEC Materials

13. Requesting Communications Security Material. CROs tell the COMSEC manager, by letter, what COMSEC materials they need to support their mission. Update the letter when there are any new requirements or changes (increase or decrease) to existing requirements (see **Attachment 3**).

13.1. CROs must review and validate their unit's COMSEC requirements (Key and Equipment) annually. After the review and validation, the CRO must provide the COMSEC manager a written list of all COMSEC requirements to include the justification (i.e., plan, regulation, operation order) for each item. If equipment is required ensure the associated instructions (KAO, KAM, etc.) issued by the COMSEC account is included.

13.1.1. Emergency material requests (less than 60 days notice before the required in-place date for physical keying materials or aids) must include a fund citation from the requesting unit to cover shipping and transportation costs.

13.2. Process requests for most COMSEC equipment through the Standard Base Supply System (SBSS). Proof of accountability that the equipment has been entered into the SBSS is required before COMSEC managers issue keying material to CROs. Requests for space and EKMS related equipments (i.e., AN/CYZ-10, KGR-96) are processed through the COMSEC account. Send a COMSEC material requirements letter to the COMSEC manager at the same time to make sure COMSEC material is on hand when required. Direct questions to your supporting COMSEC manager.

14. 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 GSA security container, vault, etc.) and take responsibility for storing and accounting for material not later than 1 duty day before the COMSEC aids' effective date.

14.1. Deploying units must take current plus 90 days of material with them. If there is a local COMSEC account to support them, turn the material over to the account, setup monthly distribution and follow their instructions. Distribution should only be changed if the unit will be deployed longer than 6 months.

15. Authorizing the Receipt and Transport of COMSEC Materials. The appointment letter authorizes the CRO and alternates to transport COMSEC materials from the COMSEC account to their duty location. Carry a copy of the appointment letter when transporting COMSEC materials.

15.1. Use of Private Vehicles. You may use private or corporate-owned vehicles to carry COMSEC material; however, notify the recipient organization of the itinerary and estimated time of arrival so that appropriate steps can be taken if the courier does not arrive on time.

15.2. Couriers. When preparing to courier classified COMSEC material, follow the requirements of AFI 31-401.

15.2.1. Specifically designate couriers for COMSEC material in writing. The authorizing official (e.g., commander) is responsible for ensuring that all couriers are properly cleared, trustworthy, and briefed on their responsibilities for safeguarding the material entrusted to them. Provide couriers instructions that cover emergency situations including loss or other compromise of the material they are carrying.

15.2.2. Couriers may hand carry keyed COMSEC equipment.

15.3. Courier Responsibilities.

15.3.1. When carrying keying material, couriers must maintain constant personal custody of all keying material entrusted to them.

15.3.2. When carrying COMSEC material couriers are responsible for ensuring the security of the material at all times. Couriers may place bulky material in a locked compartment using last-in first-out procedures if the carrier restricts access to the lock combination or key to authorized couriers. Couriers must ensure the material is given the maximum protection possible during transit and is not left unattended on loading docks, in cargo storage areas, baggage areas, etc .

15.3.3. Couriers must ensure that all inspections are conducted in their presence, and only by authorized airport security personnel. External viewing and standard airport x-raying of equipment and protectively packaged keying material is permitted. In no case will US COMSEC material be entered into foreign distribution channels unless NSA has granted prior authorization.

15.3.4. Couriers need not be armed unless local conditions deem it advisable by the commander.

15.4. Security Requirements for Airdrop. Do not fly COMSEC material over hostile territory unless it is operationally necessary. When transporting or airdropping COMSEC material over hostile territory in support of tactical operations, observe the following safeguards:

15.4.1. Do not airdrop COMSEC material unless there is a high probability of the material's immediate recovery by authorized personnel.

15.4.2. Keep COMSEC material to be airdropped under the control of a properly cleared individual until the material leaves the aircraft .

15.4.3. You may use helicopter sling-loading techniques to transport vehicles or shelters in which COMSEC equipment is installed.

15.4.4. Do not sling-load COMSEC keying material and publications, but they may be carried inside the same helicopter that is transporting the equipment .

15.5. Action Upon Receipt. Inspect packages for damage, evidence of tampering, or penetration immediately upon receipt .

16. Issuing to Communications Security Users.

16.1. Fixed COMSEC 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.

16.1.1. Normally issue users no more than 1 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 supply. See **Attachment 7** for handling instructions for keytapes.

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

16.2. Issuing to Aircrew Users. You may issue complete canisters of key for use on aircraft, however, return all unused key to the issuing CRO upon mission completion. Prior to issue:

16.2.1. Page check and seal documents (i.e., code books, authenticators, etc.). Seal documents by using a **white address label (or similar label) around one of the nonbound ends (right side, top or bottom). Initials would then be written over the label and on to the document to detect tampering or usage**. Issue the sealed document and disposition record card 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 immediately after supersession and annotate this destruction on the DRC provided destruction facilities are available. If destruction facilities are not available, hold material until the aircrew arrives at a location where destruction facilities are available.

16.2.2. When possible, issue keys electronically in a data transfer device (DTD). If physical key must be issued, issue key tape canisters in their entirety to include its associated disposition record card or appropriate form. Before issuing key canisters, the CRO will remove and destroy all superseded material. Aircrew members must destroy any key tape segments removed from the canister immediately 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.

16.2.3. Issue material in a communications (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. RON storage locations will sign “only” for the sealed kit via AF Form 12, **Accountable Container Receipt.** Ensure personnel manning storage locations at RON location are instructed to retain the sealed kit and reissue it to the same aircrew. RON storage locations are not to reissue material to other aircrews.

16.2.4. Ensure users maintain strict accountability and destroy superseded keys within established time frames. When issuing ALC-1 COMSEC aids directly to in-transit aircrews whose mission **does not** allow for the return of the material, disposition record card, or destruction certificates to the issuing office, annotate the receipt (SF 153 or AFCOMSEC 1, **COMSEC Users Receipt/ Destruction Certificate [PA]**) 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 as the destruction certificates. This is a procedure commonly referred to as "presumed destruction" and pertains only to in-transit aircrews. The Air Force still expects in-transit aircrews to properly handle, protect, and destroy COMSEC aids even though they do not tell the issuer how they disposed of them. ***NOTE:*** No matter how long the length of the TDY/deployment, deploying aircrews that 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.

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

16.3.1. Aircrews may carry complete canisters of keytapes or keylists (current plus 3 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 immediately after supersession provided destruction facilities are available. If destruction facilities are not available, hold the superseded material until the aircrew arrives at a location where destruction facilities are available.

16.4. Aircrews must make every effort to destroy and record destruction of obsolete or superseded material during intermediate stops. If destruction facilities are not available, hold superseded material

until the aircrew arrives at a location where destruction facilities are available. Destruction facilities are normally available at secure storage facilities such as base operations, network control 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 reduce the possibility of lost material.

16.5. Requirements for Aircraft Containing COMSEC Material. Due to space limitations, it is not always possible for US guards to accompany a flight. When aircrew's layover in nonallied countries and US guards are not available, aircrews must attempt to transport classified keying material to a US facility for secure storage. If this is not possible, COMSEC material may remain onboard the aircraft provided the following requirements are strictly adhered to. Use guards employed by the host country for area control only.

16.5.1. Zeroize the COMSEC equipment unless the equipment is filled with encrypted key, then remove the crypto-ignition key (CIK) or configure the equipment so that unauthorized personnel cannot operate it.

16.5.2. Crewmember will destroy or remove from personal custody all superseded keying material and keying material that is not protectively packaged.

16.5.3. Secure all remaining keying material in a container that is mounted in or internally chained to the aircraft structure.

16.5.4. Lock the aircraft and the container. If the aircraft is not lockable, then seal the doors. US personnel must check the aircraft and container the first duty hour after crew rest for signs of tampering or penetration. Report any suspected tampering according to AFI 33-212.

16.6. Handling and Controlling of Sensitive Compartmented Information (SCI) Keying Material. Any segment pulled from its canister and loaded for encryption must be treated as SCI and destroyed immediately inside a Sensitive Compartmented Information Facility (SCIF). Store segments remaining inside the canister within a SCIF. Whenever possible, use electronic key rather than paper tapes. Retention of used paper tape key segments is not recommended unless the exposed key segments are retained in NSA protected packaging. Key segments inside a canister that have never been used and become superseded must be pulled for destruction while in a SCIF. DTDs loaded with SCI keying material must be stored in a SCIF, in an approved Top Secret safe separate from the CIK. The CIK must be stored under Two Person Integrity (TPI). Load SCI keying material segments into a KYK-13 while in a SCIF and destroy the exposed segment immediately.

Section E—Physical Security Requirements for Communications Security Operations

17. Physical Security Requirements. The Air Force does not prescribe construction of special areas for storing and using COMSEC material. However, areas where open storage is required must meet the storage and other physical security requirements for the particular classification level of the COMSEC material. When a facility is approved for open storage, ensure certification by the local security forces is on file. All activities that use COMSEC materials must practice sound operations security.

18. Access Controls and Procedures. Only U.S. citizens, whose official duties require it, may access keying material and equipment, except those specifically authorized for release to allies. Access to certain COMSEC material and equipment may require enrollment in the CAP. Consult the COMSEC manager and refer to AFI 33-210 for specific CAP requirements.

18.1. CROs must only give persons with appropriate final clearance and the need-to-know access to COMSEC material.

18.1.1. For keying material, persons must have a final security clearance equal to or higher than the classification level of the keying material involved.

18.1.2. For keyed or unkeyed equipment, persons must have a final security clearance equal to or higher than the classification level of the equipment or of the keying material, whichever classification is higher.

18.1.3. For TOP SECRET keying material, **Section H** applies.

18.2. 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. (i.e., removing keying material from canisters, loading cryptographic equipment, destroying keying material, etc.).

18.3. Limit 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, rank, full SSN, and clearance levels of all persons who have COMSEC responsibilities in the facility, and may include the unit commander and supervisors. All personnel on the list must have a final security clearance equal to or higher than the COMSEC information to which they have access. All personnel listed on the access list must have completed COMSEC training before being allowed access to the COMSEC material. Refer to AFI 31-501, *Personnel Security Program Management*, for processing of security clearances.

18.4. Verify personal clearance status from the currently approved security clearance verification roster, and that the person's need-to-know exists. CROs must review the authorized access list monthly to ensure its accuracy and then annotate the review date, month, and their initials on the list. Maintain only the most current access list. ***NOTE:*** The authorizing official (for FAA, Facility Manager; for contractors, Facility Security Officer) or CRO signs the authorized access list. Get security clearance information for civilian personnel (including DoD and civil agency contractors) from the base security forces office or other knowledgeable security offices.

18.5. 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.

18.6. Record the arrival and departure of all persons not named on the authorized access list, using AF Form 1109, Federal Aviation Administration (FAA) Form 1600-8 (for FAA use only), or a local company form (for CRO contractors with COMSEC managers approval). For COMSEC users in controlled areas, keep an additional separate visitor register to record access to COMSEC material. Retain the AF Form 1109, FAA Form 1600-8 (for FAA use only), or company form on file for 1 year after date of last visitor recorded on the form.

19. Storing Communications Security Information and Material. "Storage" as used here means using security containers, vaults, alarms, guards, and so forth, to protect classified COMSEC information and material during nonworking 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 00-20F-2) to store COMSEC material.

19.1. 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 in one of the following manners :

19.1.1. TOP SECRET:

19.1.1.1. A GSA-approved, Class 6 and above, steel security container from the Federal Supply Schedule .

19.1.1.2. A Class A vault.

19.1.1.3. An area under continuous surveillance by guards.

19.1.2. SECRET:

19.1.2.1. Same as paragraph **19.1.1.**

19.1.2.2. In a Class B vault.

19.1.3. CONFIDENTIAL:

19.1.3.1. Same as paragraphs **19.1.1.** or **19.1.2.**

19.1.3.2. In a secure room.

19.1.3.3. Minimally, in a standard field safe.

19.1.4. UNCLASSIFIED CRYPTO:

19.1.4.1. Same as paragraphs **19.1.1.**, **19.1.2.**, or **19.1.3.**

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

19.2. 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 CCI, protect it by :

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

19.2.2. Do not store 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. Store the DTD with the CIK removed and place the DTD on the COMSEC inventory. Store the CIK separate from the DTD by the most secure means available to prevent unauthorized access. When the CIK is inserted, protect the DTD according to the highest classification level of key it contains.

19.2.3. 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.

19.3. Other COMSEC Material. Safeguard material other than those that paragraphs **19.1.** and **19.2.** 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, or safe combinations and 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. Request a waiver for deviations from this paragraph through MAJCOM COMSEC channels to HQ AFCA/WFP.

19.4. Lock Combinations. Unique combinations will be used for each security container (or locking drawer). Combinations will not duplicate a combination selected for another lock within the facility. Do not use easily deciphered numbers (e.g., unit designations, phone numbers, birthdays, etc.) within the combination .

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

19.4.1.1. At least once a year (every 6 months for International Pact Organization and Chairman of the Joint Chief of Staff Instruction (JCSI) 3260.1 (S) *Policy Governing JCS Material* (U).

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

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

19.4.1.4. When the combination is compromised.

19.4.1.5. When any repair work has been performed on the combination lock.

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

19.4.3. Store and file safe combinations by:

19.4.3.1. Completing SF 700 per the instructions on the form.

19.4.3.2. Choosing a location that allows ready access in an emergency but is restricted to persons with proper clearance and the need-to-know. Do not store lock combinations in contingency communications facilities .

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

19.4.4.1. Complete an Air Force Technical Order Form 36, **Maintenance Record for Security Type Equipment** .

19.4.4.2. Assign an identification number and clearly label the vault or container by permanently affixing it with the number .

19.4.4.3. Attach an SF 700 to the inside of each locking drawer of each GSA-approved container or vault. For safes or vaults having more than one lock, prepare an SF 700 for each lock. For safes or vaults having an electronic lock using the dual access mode prepare an SF 700 for each combination.

19.4.4.4. 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 nonapproved GSA security containers.

19.5. Access Control Devices (Cipher Locks or Magnetic Strip Card Locks). Use these devices only for convenience. They offer 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 monthly, when personnel knowing the combination no longer

require access to the facility, or when their access is suspsended/revoked. Clean the buttons monthly to prevent body oils and dust build-up on the numbers. Document the cleaning and changing of access control devices.

20. Security Checks. A required security check at the end of each workday (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:

20.1. All COMSEC material is properly safeguarded.

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

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

20.4. Alarms are set.

20.5. Perform daily security checks in areas containing:

20.5.1. Classified installed or stored COMSEC equipment.

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

20.5.3. COMSEC materials in high-risk environments.

20.5.4. 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 .

20.5.5. COMSEC equipment using removable CIKs (i.e., KG-95, KG-194, STU-III, etc.) have their CIKs properly secured, appropriate to the work center's storage requirements.

20.6. Record the security checks on either the SF 701 (for daily operations) or DD Form 1753, **Master Station Log** (for 24-hour operations).

20.6.1. Do not laminate or place the SF 701 behind a glass frame. The markings on the form must be made in ink directly on the form.

Section F—Safeguarding and Controlling

21. Inventory and Accounting Requirements.

21.1. All user activities with ALC-1, ALC-2, ALC-6, and classified ALC-7 material must conduct daily or shift inventories per ALC requirements. (See paragraph **10.** for detailed explanation of ALCs.)

21.2. SF 153 Hand Receipts. Account for all items from date of receipt until date of destruction or return to the COMSEC account. Maintain the original hand receipt at the COMSEC account and provide a copy to the user. Destroy the hand receipt when a properly executed local destruction certificate is received from the user or the material is returned to the COMSEC account. When multiple items are listed on a hand receipt, line through, initial, date and list disposition of items in the "Remarks" column as they are returned to the account or destroyed. Periodically consolidate hand receipts as they become messy or when an individual who has signed for the material is no longer a CRO or alternate .

21.3. 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. Only one short title may be entered per line. Multiple items of a single short title may be placed on one line if they are the same editions, and their registry numbers are sequential, otherwise use multiple lines for different editions or nonsequential ACN. Mark the inventory "FOR OFFICIAL USE ONLY" on the top and bottom of each page.

21.4. Inventory the items listed and indicate on the form that the inventory is complete. Annotate each block by marking it with an "X." The inventory includes accounting for individual segments, tapes, tables, etc., by checking the material on hand against disposition and destruction records cards.

21.4.1. Use black ink when making entries on the inventory (AFCOMSEC Form 16). Entries are considered annotating the material with an "X" and individual's initials on the bottom of the form. Do not use correction fluid, correction tape, or erasures on the form. For corrections, draw a single line through the error, initial, and number the error in the margin next to the error. On the back of the form, include the error number, date discrepancy was discovered and corrected, detailed description of the discrepancy, and the initials of the individual who made the corrections.

21.4.2. Use a specific color when removing an item from the AFCOMSEC Form 16. Block out the remainder of that entry, date, initial, and explain the reason for removal (e.g., Returned to account, Destroyed voucher number ##, etc.) When deleting a single item from a multiple line entry, completely remove the item from the inventory and readd the remaining items to the end of the inventory as a new entry.

21.4.3. Use a specific color when adding items to the AFCOMSEC Form 16. Block the entry up to the date added, date, initial, and explain the reason for the addition (e.g., Received from account, etc.) If a new inventory is printed out, identify items added on the new inventory.

21.5. For items that are continually issued outside the CRO's responsibility and then returned at a later date, (Combat Crew Comm, Base Operations issuing to aircrews, etc.,) annotate the AFCOMSEC Form 16 one of two ways:

21.5.1. For multiple entry items, completely remove the item from the inventory and when returned, annotate this return as a new entry on the inventory.

21.5.2. For single entry items, 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 (X). When using this method, list items individually on the inventory by short title, edition, and ACN (one item per line entry).

21.5.3. 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 1 day. Provide inventories to the CRO upon mission completion. File these inventories with the other inventories for the month and retain for 6 months.

21.6. 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.

21.6.1. Do not open security containers on a daily basis for the sole purpose of inventorying the contents; only open when needed. Perform an inventory each day the container is opened just prior to final closing.

21.7. 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 access. Prepare as many separate inventories as necessary.

21.8. Part-time facilities perform an inventory on opened safes upon closing the facility.

21.9. Sealed packages containing COMSEC materials 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 the package number on AFCOMSEC Form 16. Mark the sealed package with the appropriate classification. Write the CRO's initials over the package's seal in such a way that tampering will be obvious.

21.9.1. Assign a unique number (i.e., 03-01 (last two digits of the year and the package number) that is not reutilized. Place this number on the outside of that package and on the internal and external AFCOMSEC Form 16.

21.9.2. Prior to sealing the package conduct an inventory and mark the inner AFCOMSEC Form 16.

21.9.3. Enter the sealed package on the AFCOMSEC Form 16 in the following manner: Short title/Edition - “Sealed Package” and the package number; Quantity will be 1 and the serial number will be left blank (e.g., “Sealed Package 03-01”)

21.9.4. Use paper tape with nylon or fiber reinforcement to seal packages.

21.9.5. When the sealed container is opened, inventory the COMSEC material inside prior to resealing.

21.10. On an AFCOMSEC Form 16, inventory classified and, or certified (e.g., KGR-96, KOK-13, etc.) 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. List DTDs on the inventory, regardless if keyed or unkeyed.

21.11. 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.

21.12. The CRO must review inventories monthly to make sure they are accomplished correctly. Document the reviews by dating and initialing the front bottom corner of the AFCOMSEC Form 16. Keep the current and the previous 6 months of inventory records on file according to AFMAN 37-139.

21.13. 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.

21.14. Notify the COMSEC manager immediately if you are unable to pull keying material from a key tape canister.

22. Page Checks of Classified Communications Security Publications.

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

22.1.1. Before initial issue to any aircrew.

22.1.2. 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, and so forth). Check that the document does not have printing or production errors. Record the page check on the record of page checks page in the basic document. Report errors to the COMSEC manager.

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

22.1.4. Prior to destruction. This page check does not have to be recorded. This is to ensure that all the pages within the document are destroyed.

22.2. The COMSEC manager and CRO must ensure completed page checks of COMSEC publications. You do not need to check pages of AFI and AFSSI publications. COMSEC managers have the right to require additional page checks as needed. Unclassified documents do not require page checks unless changes are made by replacing pages.

22.3. Make page checks by:

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

22.3.2. Checking that each page is exactly as described.

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

22.3.4. Annotate the date and signature of the person making the check.

23. 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.

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

23.1.1. One person adds the new pages and also:

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

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

23.1.2. A second person:

23.1.2.1. 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, Amend 1, Amend 2, etc.). A document can be numbered correctly even

though it contains old pages that should have been replaced by new pages.

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

23.2. Users amend publications they have received. COMSEC account personnel make amendments changes to publications held at the COMSEC account.

24. Accounting For and Disposing of Amendments.

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

24.2. The COMSEC manager will either direct 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.

24.3. The agency entering an ALC-4 amendment destroys the pages according to **Section G** after the second person performs a page check.

25. Photography.

25.1. Do not take photographic equipment into areas where keying material is exposed or visible. Secure all keying material in locked containers prior to allowing photographic equipment into the area.

25.2. Do not allow photographs of equipment internals to be taken; however, official photographs of equipment externals are permissible. Official or unofficial photographs, drawings, or descriptive information for press release or private use are prohibited.

25.3. Aircraft commanders are responsible for control of photographic equipment on board aircraft that contains COMSEC material. Carefully monitor unofficial photography so as not to permit photographs of COMSEC equipment or operations by limiting the area or panels photographed or by covering the equipment.

26. Public Display of COMSEC Material. COMSEC equipment and ancillary devices may be displayed at official functions such as symposium, open houses, etc., if in the opinion of the commander, there are sufficient procedures in place to reasonably preclude theft, tampering, unauthorized access, etc. Key equipment used for demonstration with only unclassified test or maintenance key.

Section G—Destruction

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

28. Routine Destruction Security. Make facilities and equipment available for routinely destroying superseded keying material and other COMSEC. You must be able to 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.

29. Scheduling Routine Destruction.

29.1. Do not destroy COMSEC material before its supersession date unless you receive proper disposition instructions (i.e., message from the controlling authority) if other than normal supersession .

29.2. Destroy used keying material designated CRYPTO as soon as possible, but immediately after supersession. See applicable AFSSI for key reuse and holding rules. Under special circumstances (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.

29.2.1. 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.

29.2.2. Do not remove keytape segments stored in canisters until just before using or destroying them. Keep unused keytape segments in the keytape canister until needed or the canister's effective period ends. If you take out any keytape segments, destroy all superseded keytape segments immediately. Exposed key tape segments must be sealed in NSA protective technology packaging or an opaque envelope sealed in such a way that tampering would be obvious (i.e., writing the signatures/initials over the seal). If material is TPI, two sets of signatures/initials are required. Annotate on the short title, ACN, segment, and quantity on the sealed envelope and store it with the canister and DRC. Use DRC 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 immediately 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 then destroy it immediately after supersession. Document unreliable circuits to the controlling authority with a letter, e-mail, or message and annotate the authority on the DRC. (3) Disposition records used for unclassified ALC-1, ALC-6, or ALC-7 keying material are UNCLASSIFIED FOR OFFICIAL USE ONLY when filled in.

29.2.2.1. When making annotations on the disposition record (e.g., AFCOMSEC Form 22B, DRC, etc.), individuals will place date, signature or initial, in each applicable block. For Top Secret keytapes two initials are required for issue to validate that TPI procedures are being followed.

29.2.2.1.1. For partial canisters: If segments 1 through 10 are used within a canister and segments 11 through 31 remain at the end of the month and must be destroyed, the remainder of the canister may be “Z”d on the DRC.

29.2.2.1.2. For entire canisters:

29.2.2.1.2.1. If no segments were issued, destroy the entire canister, complete an SF-153 only, annotate after the “Nothing Follows” – “No segments issued” and both the destruction official and witness will initial next to the statement. No DRC is required.

29.2.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, com-

plete an SF-153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement.

29.2.2.1.2.3. If all segments are loaded into a DTD and the segments need to be retained, (circuit must be unreliable and you must have something from the controlling authority stating to retain keying material) seal the segments in NSA protective packaging or an opaque envelope where tampering is evident. Superseded key must be destroyed during the month if the material locked in a safe is accessed during the month. Annotate the DRC the same as partial canisters.

29.2.3. Keep pages, tables, and day sheets from codes and authenticators, if not removed, in the document until the document's effective period ends. If pages have been removed, immediately destroy all superseded pages. Record the destruction of individual pages, tables, day sheets, and so forth, from codes and authenticators on the destruction record page in the document (if provided), an SF-153, or an AFCOMSEC Form 1.

29.2.4. Destroying COMSEC material. Prepare a destruction certificate (SF-153) for all ALC-1, ALC-6, and classified ALC-4 and ALC-7, COMSEC aids authorized to be destroyed.

29.2.4.1. List the material alphanumerically by short title, edition designator, and accounting control numbers (if applicable).

29.2.4.2. After the "NOTHING FOLLOWS," enter the authority for destruction (Message Authority, etc.) if the destruction authority is other than normal supersession.

29.2.4.3. Before destroying, both the destruction and witnessing official must verify the short title, edition, quantity, and accounting control number(s) of each item listed on the destruction certificate.

29.2.4.4. Make corrections to destruction certificates with a single line through the error, and initialed by both the destruction and witnessing officials.

29.2.4.5. Prepare the destruction certificate prior to destruction, but the destruction and witnessing official do not sign the certificate until destruction is finished and the area has been checked to ensure destruction is complete.

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

29.4. Destroy superseded general COMSEC documents (i.e., AFKAGs, KAOs, KAMs, etc.) within 5 calendar days from the supersession date.

29.5. Destroy the remains of amendments you have made to classified COMSEC publications within 5 calendar days after making the amendment change.

29.6. Destroy compromised material immediately after you receive disposition instructions or upon receipt of case closure from AFCA.

29.7. 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, or an AFCOMSEC Form 1.

29.8. Destroy correspondence relating to superseded documents when it is no longer valuable .

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

30.1. 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 .

30.1.1. 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.

30.1.2. When pulping or pulverizing paper COMSEC aids, break the material into bits no larger than five millimeters.

30.1.3. Key tapes are paper-mylar-paper. The only approved methods for destroying key tapes are by a disintegrator, burning, or pulverizing. Do not place keying material in burn bags for destruction along with other classified waste.

30.1.4. NSA approves destruction devices used for destruction of COMSEC material. Consult the COMSEC manager for a listing of NSA-approved destruction device listing.

30.2. 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 melting, pulverizing, and chemical alteration.

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

30.3. Plastic Canisters. The goal of destroying the plastic canister is to ensure no keytape segments remain in the empty plastic canisters. Remove the barcode sticker from the canister and destroy the sticker by shredding prior to destroying the canister. Crush the sides of the canister with a hammer or blunt instrument. Take safety precautions to prevent injuries caused by the shattering canister.

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

31. 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:

31.1. The destruction official is an appropriately cleared, responsible individual. The destruction official will be physically present and perform the destruction of the material listed in the destruction report. ***NOTE:*** Since there is no formal grade requirement, CROs must ensure officials are trustworthy and knowledgeable.

31.2. The witnessing official must have a clearance consistent with the material being destroyed. The witnessing official will be physically present and view the destruction of the material listed in the

destruction report. 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.

31.3. Sign the destruction report by the destruction official and the witnessing official once the destruction is complete and they have checked the destruction machine and area for residue. Destruction reports will never be signed in advance of the actual destruction by either the destruction or witnessing official. Ensure all destruction requirements set by this instruction are met before signing the destruction report.

32. 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 .

32.1. Disposal of ALC-1, ALC-6 and ALC-7 materials:

32.1.1. Use the DRC provided to record destruction of each key setting. Destroy unused key, pages, tables, or day sheet, etc., when you load a current one or immediately after supersession.

32.1.2. Provide a copy of all completed destruction records (SF 153) to the COMSEC account no later than the first duty day after the material supersession. The CRO will attach the completed DRCs to the applicable SF 153. These may be maintained by the CRO or the COMSEC account; it is the COMSEC Manager's choice. When the DRCs are attached the SF 153 becomes CONFIDENTIAL.

32.1.3. Maintain the original completed disposition and destruction record on file for 3 years from the date of destruction according to AFMAN 37-139.

32.1.4. For items issued to transient or deploying aircrews not returning to your location, file a copy of the signed, annotated receipt and keep it for 3 years after the yearly cutoff. Returning aircrews must immediately give unused material and DRC to their CRO.

32.2. Disposal of ALC-4 Material:

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

32.2.2. When the COMSEC manager directs, destroy the material, record destruction of classified documents on a SF 153, and keep the destruction certificate for 3 years according to AFMAN 37-139.

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

Section H—Control of TOP SECRET Keying Material

33. 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; therefore, 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.

34. Exceptions. This section does not apply to:

34.1. Sealed Authenticator System (SAS) and Permissive Action Link (PAL) material.

34.2. 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.

34.3. 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).

35. Two-Person Integrity (TPI) 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 develops and uses procedures and controls to make sure lone individuals do not have access to TOP SECRET keying material (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.).

36. Transportation. Follow these procedures for moving TOP SECRET keying material:

36.1. Local transport of TOP SECRET keying material:

36.1.1. 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. ***NOTE:*** A KSD-64A is NOT protective packaging. KSD-64As loaded with operational TOP SECRET keying material and not wrapped in protective packaging (pink plastic wrapper) must be protected under TPI.

36.1.2. Locally transporting TOP SECRET keying material in NSA-approved protective packaging (key canisters, pink plastic wrapper, etc.) 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 an individual picks up the material from the COMSEC account, they must inspect the package for tampering and record the inspection on all copies of the hand receipt from the COMSEC account. When the material is delivered 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.

36.2. Consult the COMSEC manager for procedures for moving TOP SECRET keying material by U.S. military or U.S. flag commercial aircraft .

37. Storing Material.

37.1. 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 X07 or X08 three-position, dial-type, combination locks that no one person can open. Use dual 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 combination must have a separate SF 702. ***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.

37.2. 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 .

37.3. TPI storage procedures are not required for TOP SECRET key in tactical situations.

37.3.1. In these situations where units are unable to meet normal TPI storage requirements must either:

37.3.1.1. Store TOP SECRET keying material in a standard, GSA-approved field safe or similar container secured by a padlock meeting Federal specification FF-P-110 .

37.3.1.2. Or, if adequate storage facilities are not available, keep TOP SECRET keying material under personal custody .

37.3.2. Procedures in effect must require inspections of protective packaging according to applicable protective technology pamphlets.

38. Use.

38.1. Establish 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* .

38.2. Set up CNLZ at user locations whenever:

38.2.1. Permuter trays are set up with TOP SECRET key, whether installed in the equipment or not.

38.2.2. Cryptographic equipment contains TOP SECRET key in hard-copy form.

39. 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 on a separate SF 700 part 2 and store each form in different approved secure containers.

40. Two-Person Integrity (TPI) 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.

41. Waivers. TOP SECRET keying material not in NSA-approved protective packaging and TOP SECRET key generators require TPI unless a waiver is granted by MAJCOM with the controlling authorities approval. 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 an approved waiver has been granted.

41.1. The CRO submits TPI waiver request through their unit commander to the COMSEC manager who will submit it to the MAJCOM. The COMSEC manager will verify that all personnel listed on the TPI waiver have cryptographic access.

41.2. MAJCOMs will verify and validate the waiver request and obtain controlling authorities approval. MAJCOMs will assign a unique case number to all waivers with the waiver type, MAJCOM, last two digits of the year, and case number within the year (e.g., TPI-AMC-03-01). Send an info copy of the waiver to HQ AFCA.

41.3. Waiver request will be for no more than 12 months. Extensions will then be considered on a case-by-case basis.

Section I—Emergency Action Plans

42. 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.

43. Emergency Protection Planning.

43.1. Activities that hold classified ALC-1, ALC-2, ALC-6, or classified ALC-7 material must develop and maintain a current EAP (see **Attachment 5**) to protect material during emergencies .

43.2. 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.

43.3. 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).

43.4. 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.

43.4.1. Encase deployed EAP cards in such a way that building/tent/facility and phone numbers for fire department, security forces, hospital/clinic, command post, etc., can be written in upon arrival at each site.

43.5. For fire, natural disaster, and bomb threat plans, keep the material secure until order returns.

43.6. 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.

44. 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.

44.1. The CRO prepares the plan since they are the person most familiar with the amount and significance of the COMSEC material on hand.

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

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

44.3.1. Duties must be clear and concise.

44.3.2. 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 .

44.3.3. Conduct and document reviews and training exercises (“dry runs”) at least every 6 months. High-risk areas practice training exercises at least every 3 months. This ensures that all persons can effectively carry out their emergency duties.

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

44.4. Planners must consider three emergency options:

44.4.1. Securing the material.

44.4.2. Removing the material from the emergency scene.

44.4.3. Destroying the material.

44.4.4. 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.

44.5. 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.

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

45.1. Classify according to subject.

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

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

45.4. Locate COMSEC material by storage containers.

45.5. Schedule dry runs.

45.6. Safeguard COMSEC material as much as possible and ensures the CRO reports the destruction of COMSEC material to the COMSEC manager.

45.7. Include on a separate card, names, addresses, and telephone numbers of all persons and organizations to contact in an emergency.

45.8. Make task cards identifying specific actions to accomplish 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.

45.9. Make coordination part of the plan. Coordinate the EAPs, in writing, with the COMSEC manager .

45.10. Review and revise the plan at least every 3 years or when significant changes occur.

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

46.1. 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.

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

46.3. 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.

46.4. Evacuating the area.

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

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

46.7. Personnel must avoid loss of life or personal injury during efforts to protect COMSEC material.

47. 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:

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

47.2. 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).

47.3. 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 .

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

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

47.6. Establishing emergency communications procedures.

48. 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:

48.1. Hold only the minimum amount of COMSEC aids.

48.2. Destroy all superseded material immediately.

48.3. 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.

48.4. For precautionary destruction, follow the priorities in paragraph **49.** However, keep the COMSEC aids necessary to maintain essential operations until you receive orders for emergency destruction. Retain :

48.4.1. All equipment.

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

48.4.3. A 60-day supply of COMSEC aids.

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

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

49. 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.

49.1. 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.

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

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

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

49.1.4. All remaining future keying material.

49.2. 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.

49.2.1. Sensitive pages of cryptographic equipment maintenance manuals.

49.2.2. Other classified documents.

49.2.3. Classified COMSEC files.

49.3. 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):

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

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

50. Combined Priority List. The priority list in paragraph **49.** 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 :

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

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

50.2.1. TOP SECRET.

50.2.2. Secret.

50.2.3. Confidential.

50.3. 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.

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

50.5. Other classified COMSEC documents.

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

50.7. Classified COMSEC files.

51. Methods and Extent of Emergency Destruction. Use any approved methods 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.

51.1. 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.

51.2. 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 Manual [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:

51.2.1. A sodium nitrate fire.

51.2.2. Incendiary cryptographic equipment destroyers.

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

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

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

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

52.2. Cold chisel: 5 3/4 inch long, 1/2-inch wide tip.

52.3. Stubby screwdriver: 1-inch blade, 7/32-inch wide tip.

52.4. Screwdriver: 1 1/2-inch blade, 5/32-inch wide tip, and 6-inch blade, 5/16-inch wide tip.

52.5. Phillips screwdriver: Numbered 0 and 2.

52.6. Wrench: 5/16 inch, box and open-end combination.

52.7. Pliers: 5-inch diagonal cutting and heavy duty, lineman.

52.8. Crowbar.

52.9. Fire ax or sledgehammer.

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

54. 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. Whenever possible, electronic copies of keys should be taken vice hard copies of keying materials. Paragraph **49.** outlines destruction priorities.

54.1. 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.

54.2. If the aircraft is over land in a friendly area, keep the crypto material in the aircraft.

54.3. 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.

54.4. Only take mission essential COMSEC material aboard an aircraft. To facilitate this process, consider the mission and length of the flight to minimize the quantity of material to destroy in an emergency.

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

55. 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. See **Attachment 6**.

Section J—Communications Security Deviations

56. Communications Security Deviations Reporting. The importance of reporting all known or suspected COMSEC deviations 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.

56.1. 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 (e.g., AFSSIs, KAOs) also list reportable incidents. Some specific actions you must report are:

56.1.1. Physical Incidents. Loss of control, theft, recovery by salvage, improper destruction, tampering, unauthorized viewing, access, or copying, and so forth.

56.1.2. 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.

56.1.3. 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.

56.2. 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.

56.2.1. The CRO advises the COMSEC manager who prepares and submits the initial incident report according to AFI 33-212 .

56.2.2. 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).

56.3. 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.

56.4. The inquiry or investigating official contacts the COMSEC manager for information and completes the inquiry or investigation report per AFI 33-212.

56.5. 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.

57. Reporting Procedures. Immediately report possibly endangered classified COMSEC aids to the CRO or COMSEC manager. Use secure communications when talking about the nature of the incident because the events surrounding a security incident may be classified.

57.1. Deployed user immediately contacts the deployed CRO who, in turn, notifies the closest COMSEC manager.

Section K—Information Assurance Assessment and Assistance Program (IAAP)

58. Communications Security Assessment and Assistance Program. The COMSEC assessment and assistance program provides an effective management tool to make sure that COMSEC procedures are properly followed.

59. Communications Security Assessment and Assistance. The COMSEC manager must conduct an assessment and audit of COMSEC user's facilities semiannually at scheduled times. Use AF Form 4160, **Section I**. 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 major command also checks these users during the periodic command Information Assurance Assessment and Assistance Program (IAAP) of the COMSEC account.

59.1. The COMSEC account notifies all CROs of the upcoming assessment/audit.

59.2. Users positively identify all COMSEC assessors by comparing the identification card (DD Form 2, **Armed Forces Identification Card [Active, Reserve, and Retired]**, Common Access Card, or Air Force Form 354, **Civilian Identification Card**) with the assessment/audit message notice, TDY orders, or records the COMSEC manager provides. Sign them in on the Air Force Form 1109 or

FAA Form 1600-8 (for FAA accounts). ***NOTE:*** Another form of ID may be needed with the CAC since SSNs are not listed on civilian or contractor CACs. Use a valid state driver license or a recent payroll statement as a second form of ID with the CAC.

59.3. The COMSEC manager and command IAAP personnel may also conduct assessments/audits without notice.

60. Information Assurance Assessment and Assistance Program (IAAP) Checklist. The COMSEC manager checks those items listed on the AF Form 4160 when conducting assessment on COMSEC materials. MAJCOMs and wings may supplement this form .

61. Wing Communications Security Assessment/Audit Procedures.

61.1. COMSEC account personnel prepare a narrative report identifying the user's rating, individual discrepancies and references, and recommend corrective actions.

61.2. Forward the report through the CRO's commander to the CRO for reply back to the COMSEC account.

61.3. 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 set by the COMSEC manager.

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

61.5. **DELETED.**

61.6. **DELETED.**

61.7. The COMSEC manager closes open items on the assessment report once the corrective action has been completed.

61.8. Keep all assessment/audit reports on file from one command assessment to the next command assessment.

61.9. If a user is rated Unsatisfactory, the wing COMSEC manager notifies the CRO's commander in person and conducts another assessment/audit within 90 days.

62. Information Collections, Records, and Forms.

62.1. Information Collections. No information collections are created by this publication.

62.2. Records: Maintain and dispose of records created by this publication according to Air Force Web-RIMS RDS, Table 33-22, Rules 1, 2.01, 2.02, 3, 5, 5.01, 6, 8, 9, and 26, located at **https://webrims.amc.af.mil/rds/index.cfm**.

62.3. Forms: (Adopted and Prescribed).

62.3.1. Adopted Forms: SF 153, **COMSEC Material Report**; SF 700, **Security Container Information**; SF 701, **Activity Security Checklist**; SF 702, **Security Container Check Sheet**; DD Form 2, **Armed Forces Identification Card (Active, Reserve, and Retired)**; DD Form 254, **DOD Contract Security Classification Specification**; DD Form 1753, **Master Station Log**; AF Form 12, **Accountable Container Receipt**; AF Form 354, **Civilian Identification Card**; AF Form 847, **Recommendation for Change of Publication**; AF 1109, **Visitor Register Log**; AF

Form 3215, **C4 Systems Requirement Document**; AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria;** AF Form 4168, **COMSEC Responsible Officer and User Training Checklist;** AFCOMSEC Form 9, **Cryptographic Access Certificate (PA)**; AFCOMSEC Form 16, **COMSEC Account Daily - Shift Inventory**; and AFTO Form 36, **Maintenance Record for Security Type Equipment.**

62.3.2. Prescribed Forms: AFCOMSEC Form 1, **COMSEC Users Receipt/Destruction Certificate** (PA).

LESLIE F. KENNE, Lt Gen, USAF
DCS, Warfighting Integration

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 104-13, *The Paperwork Reduction Act of 1995*

AMSG-293, *NATO Cryptographic Instruction*

AMSG-773, *Policy and Procedures for Handling and Control of Two-Person Controlled (TPC) NATO Sealed Authentication System (SAS)*

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

CJCSI 3260.01, *Policy Governing Positive Control Material*

AFPD 33-2, *Information Protection (*will become *Information Assurance)*

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

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-210, *Cryptographic Access Program*

AFI 33-212, *Reporting COMSEC Deviations*

AFI 33-230, *Information Protection Assessment and Assistance Program (*will become *Information Assurance Assessment and Assistance Program)*

AFI 33-275, *Controlled Cryptographic Items*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFMAN 23-110, *USAF Supply Manual*

AFMAN 33-272, (S) *Classifying COMSEC and TEMPEST Information* (U) (will become *Classifying Information Assurance Information (U)*)

AFMAN 37-123, *Management of Records*

AFMAN 37-139, DELETED

AFDIR 33-303, *Compendium of Communications and Information Technology*

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

AFKAG-2, *Air Force COMSEC Accounting Manual*

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

Web-RIMS, *Records Disposition Schedule (RDS)*

Abbreviations and Acronyms

ACN—Accounting Control Number

AFCA—Air Force Communications Agency

AFCOMSEC—Air Force Communications Security

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Manual

ALC—Accounting Legend Code

CAP—Cryptographic Access Program

CCI—Controlled Cryptographic Item

CIK—Crypto-Ignition Key

CJCSI—Chairman of the Joint Chief of Staff Instruction

CMCS—COMSEC Material Control System

CM^2—Computerized Management of COMSEC Material

CNLZ—COMSEC No-Lone Zone

COMSEC—Communications Security

CONUS—Continental United States

COR—Central Office of Record

CRO—COMSEC Responsible Officer

DRC—Disposition Record Card

DRU—Direct Reporting Unit

DTD—Data Transfer Device

EAP—Emergency Action Plan

EKMS—Electronic Key Management System

EOM—End of Month

FAA—Federal Aviation Administration

FOA—Field Operating Agency

GS—General Schedule

GSA—General Services Administration

IAAP—Information Assurance Assessment and Assistance Program

MAJCOM—Major Command

NATO—North Atlantic Treaty Organization

NSA—National Security Agency

OI—Operating Instruction

PAL—Permissive Action Link

PROM—Programmable Read-Only Memory

RDS—Records Disposition Schedule

RON—Remain Overnight

SAS—Sealed Authenticator System

SBSS—Standard Base Supply System

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SF—Standard Form

SSN—Social Security Number

STU—Secure Telephone Unit

TDY—Temporary Duty

TPI—Two-Person Integrity

UCM^2—Users Computerized Management of COMSEC Material

URL—Uniform Resource Locator

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, and so forth, marked CRYPTO), call sign 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.

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 (COR), 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.

Electronic Key Management System (EKMS)—Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generation, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

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 materials (*identify unit and office symbol*). Appointees can receive and carry all COMSEC materials issued, up to and including the classification indicated directly between _____ (*COMSEC account*), Building _____ and _____(*user location building number*). They will make sure the materials they receive are entered on their daily inventory and are responsible for their safekeeping and for other actions required of users of COMSEC materials by AFI 33-211. These individuals have been granted access to classified COMSEC information and appropriate documentation is on file. These individuals have also been appointed as CAP Administrators according to AFI 33-210.

RANK/NAME	SSN	CLEARANCE	DUTY PHONE	AFTER-HOURS PHONE

2. Please brief and train the newly appointed individuals per AFI 33-211.

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 (for example: "HQ AFCA requires material in support of Operation Plan (OPLAN), JCS Exercise_____, and so forth" General statements, such as "to fulfill mission requirements" or "as directed by XYZ message 091234Z Jan 02," are not accepted by themselves; we need further justification.)

3. Attached is proof that the equipment has been entered into the Standard Base Supply System according to AFMAN 23-110.

(*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 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

A5.1. Fire Task Cards.

EXAMPLE - Task Card #1:

-- Purpose. Provides for orderly evacuation of personnel and protection of COMSEC material within facilities using COMSEC aids and equipment in case of fire.

-- The senior person present implements the plan by issuing task cards. If a limited number of personnel are available to carry out each task, combine the tasks.

-- After the fire is out, inspect the safes for signs of entry or tampering and take a complete inventory of all COMSEC material.

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

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

EXAMPLE - Task Card #2.

-- Sound alarm and notify Fire Department, stating: **THIS IS** (*Rank/Name*)**,**
REPORTING A FIRE IN BUILDING _____, ROOM _____.

-- Do not hang up the telephone until the fire dispatcher knows the location and has no questions.

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

EXAMPLE - Task Card #3.

-- Secure all COMSEC material (keytapes, keylists, code books, Data Transfer Device (DTD), and so forth), the STU-III keys, and all other classified material in the safe along with COMSEC inventories.

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

EXAMPLE - Task Card #4.

-- Fight any open fire, if possible, using available fire extinguishers.

-- Fire extinguisher(s) (*Type*) is/are located _____(*where*)_____.

EXAMPLE - Task Card #5.

-- Open and guard the door that gives fire department personnel greatest access to the fire.

-- Admit all firefighting personnel, including local national firefighters.

EXAMPLE - Task Card #6.

-- Notify the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- Manager, COMSEC account _____ (duty hour phone number _____ and non-duty hour phone number _____).

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

EXAMPLE - Task Card #7.

-- Take names of all Fire Fighters for inadvertent oath, if necessary.

-- Take inventory to ensure all material is present.

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

A5.2. Natural Disaster Task Cards :

EXAMPLE - Task Card #1.

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

-- 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 are available to carry out the tasks, combine the tasks.

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

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

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

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

EXAMPLE - Task Card #3.

-- If time and circumstances permit, destroy all superseded COMSEC material and annotate the destruction.

EXAMPLE - Task Card #4.

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

A5.3. Bomb Threat Task Cards :

EXAMPLE - Task Card #1.

-- Purpose. To protect COMSEC material in facilities using COMSEC materials in the event of a bomb threat.

-- 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 are available to carry out the tasks, combine the tasks.

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

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

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

EXAMPLE - Task Card #2.

-- Notify the Security Forces.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

EXAMPLE - Task Card #3.

-- Gather and secure all COMSEC material (keytapes, keylists, code books, DTD, etc.), the STU-III keys, and classified material in the safe along with the COMSEC inventories.

-- Leave the building and go to the designated assembly point located (enter location).

EXAMPLE - Task Card #4.

-- Conduct a search of the area and look for suspicious objects.

-- If found, guard the entrance and admit only authorized personnel until security police take over.

-- If not found, leave the building and go to the designated assembly point located (enter location).

A5.4. Emergency Evacuation Task Cards :

EXAMPLE - Task Card #1.

-- Purpose. To protect COMSEC material in facilities using COMSEC aids and equipment during emergency evacuation.

-- 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 are available to carry out the tasks, combine the tasks.

-- After the emergency, completely inventory all COMSEC material.

-- If you suspect tampering or damage, thoroughly page check all COMSEC items.

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

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

EXAMPLE - Task Card #3.

-- If time permits, destroy all superseded COMSEC aids.

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

EXAMPLE - Task Card #4.

-- Gather all current material required for immediate secure communications, as well as the COMSEC inventory, and put them in a canvas bag.

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

EXAMPLE - Task Card #5.

-- Remove COMSEC aids in use from all COMSEC equipment and put them in a canvas bag.

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

EXAMPLE - Task Card #6.

-- Secure the facility as well as possible so forced entry will be obvious.

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

EXAMPLE - Task Card #7.

-- If you expect to evacuate for a short time, secure all other COMSEC items (including future COMSEC aids) in an approved storage container.

-- Put material required to maintain secure communications in a canvas bag.

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

EXAMPLE - Task Card #8.

-- Evacuate the material, under constant surveillance, preferably by authorized personnel, to the designated evacuation site and begin secure communications.

A5.5. Emergency Destruction Task Cards

A5.5.1. Phase I--Precautionary Destruction Task Cards:

EXAMPLE - Task Card #1.

-- Purpose: To provide guidelines for:

--- Destroying COMSEC material during emergencies resulting from natural, accidental, or hostile causes.

--- Reducing holdings as a precautionary measure.

--- Preventing their capture or compromise in an actual emergency or attack.

-- Personnel authorized to implement this plan:

--- Commander (applicable unit).

--- Commander (issuing COMSEC account unit).

--- Manager, COMSEC account.

--- CRO or alternate.

--- Senior member present.

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

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

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

EXAMPLE - Task Card #3.

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

-- 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.

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

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

EXAMPLE - Task Card #4.

-- Go to the incinerator in Building _____ and fire it up.

-- The material for destruction is brought to you.

-- Place it in the incinerator as you receive it.

-- Tend the incinerator until all material is burned.

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

EXAMPLE - Task Card #5.

-- Gather all superseded COMSEC aids, using the attached Priority of Destruction list, and place in canvas bags.

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #6.

-- Gather all future COMSEC aids (those not scheduled to go into effect within the next 60 days), using the destruction priority listing, and place in canvas bags.

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #7.

-- Gather all administrative documents, files, training aids, and other material not required for continued operations and place in canvas bags.

-- Take the bags to the incinerator for destruction.

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

A5.5.1.1. Phase II--Total Emergency Destruction Task Cards:

EXAMPLE - Task Card #1.

-- Purpose: To provide guidance for preventing capture or compromise of COMSEC material in an actual emergency or attack.

-- 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.

-- After emergency destruction or as soon as possible if emergency destruction is not completed, record all destruction on the preaddressed emergency destruction letter and carry it to the COMSEC manager.

EXAMPLE - Task Card #2.

-- Notify the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

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

EXAMPLE - Task Card #3.

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

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

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

EXAMPLE - Task Card #4.

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

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

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

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

EXAMPLE - Task Card #5.

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

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

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #6.

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

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #7.

-- Remove all classified and Controlled Cryptographic Item (CCI) boards from the COMSEC equipment, thoroughly smash them with a hammer or an ax, and scatter the pieces.

-- Document destruction on the COMSEC inventory (AFCOMSEC Form 16).

-- Write names of unlisted items on the back of the form.

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

A5.6. 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.

A5.6.1. Keying Material.

A5.6.1.1. All superseded keying material and future editions of sealed authenticator system (SAS) and permissive action list (PAL) material:

A5.6.1.1.1. TOP SECRET (shared material ahead of point-to-point).

A5.6.1.1.2. SECRET (shared material ahead of point-to-point).

A5.6.1.1.3. CONFIDENTIAL (shared information ahead of point-to-point).

A5.6.1.2. All current keying material (zeroize all cryptographic equipment and remove and destroy current keylists and keytapes).

A5.6.1.2.1. TOP SECRET (shared information ahead of point-to-point).

A5.6.1.2.2. SECRET (shared information ahead of point-to-point).

A5.6.1.2.3. CONFIDENTIAL (shared information ahead of point-to-point).

A5.6.1.3. All future keylists, keytapes, codes, and authenticators scheduled to take effect within the next 30 days:

A5.6.1.3.1. TOP SECRET (shared information).

A5.6.1.3.2. SECRET (shared information).

A5.6.1.3.3. CONFIDENTIAL (shared information).

A5.6.1.4. All remaining future keying material.

A5.6.2. COMSEC Documents.

A5.6.2.1. Sensitive pages of cryptographic equipment maintenance manuals.

A5.6.2.2. Remaining classified documents.

A5.6.2.3. Classified COMSEC files.

A5.6.3. Cryptographic Equipment.

A5.6.3.1. Remove and destroy (time permitting), and list location.

A5.6.3.1.1. Readily removable classified and sensitive CCI elements.

A5.6.3.1.2. 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*)
(Typed Name, Rank, Branch of Service)

_____

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

_____

Date of Destruction

Attachment 7

HANDLING INSTRUCTIONS FOR ALL KEYTAPES

A7.1. Do not remove keytape segments until immediately prior to use or destruction. DO NOT REMOVE TAPE SEGMENTS FOR INVENTORY. If a tactical user requires more key than can be set or electrically stored in the crypto-equipment, the user may furnish additional key in electrical form in a common fill device or in hard copy form in a tape canister. Do not issue tape segments as extracts.

A7.2. Maintain the applicable disposition record card (DRC) for each keytape canister. Retain completed DRC and attach it to the local destruction report (SF 153).

A7.2.1. When making annotations on the DRCs, individuals will place date, signature or initial, in each applicable block. For Top Secret keytapes two initials are required for issue to validate that TPI procedures are being followed.

A7.2.1.1. For partial canisters: If segments 1 through 10 are used within a canister and segments 11 through 31 remain at the end of the month and must be destroyed, the remainder of the canister may be "Z"d on the DRC.

A7.2.1.2. For entire canisters:

A7.2.1.2.1. If no segments were issued, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" – "No segments issued" and both the destruction official and witness will initial next to the statement. No DRC is required.

A7.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement. No DRC is required.

A7.2.1.2.3. If all segments are loaded into a DTD and the segments need to be retained, (circuit must be unreliable and you must have something from the controlling authority stating to retain keying material) seal the segments in NSA protective packaging or an opaque envelope where tampering is evident. Superseded key must be destroyed during the month if the material locked in a safe is accessed during the month. Annotate the DRC the same as partial canisters.

A7.3. COMSEC managers may destroy segments of unissued tapes as they are superseded or may destroy unissued tapes as whole editions.

A7.4. Some key that is designated for off-the-air use (e.g., maintenance, test, classroom training, and demonstrations) has no prescribed cryptoperiod and may be used until no longer serviceable and then destroyed.

A7.5. Reproduction of associated tape is prohibited without the approval of the controlling authority.

A7.6. Notify the controlling authority immediately if the associated tape is lost, subjected to unauthorized viewing, or possibly compromised in any way. Report any incident according to AFI 33-212.

A7.7. Canister Disposition Instructions: Remove barcode stickers and destroy as classified trash. Once the key has been superseded and removed from the canister, destroy both large flat surfaces of the canister. The destruction of the canister requires that you follow the DESTRUCTION PROCEDURE below, and in addition, apply the proper SAFETY PROCEDURES at the time of destruction.

A7.8. Safety Procedures. An empty tape canister will shatter if fractured with a blunt instrument. To protect from possible injury due to flying fragments, place the canister inside a zip-lock plastic bag or similar sealable bag before beginning the destruction procedure. Wear protective eyewear during the destruction procedure to prevent injury.

A7.9. Destruction Procedure. Place the canister inside a zip-lock plastic bag or similar sealable bag, and set it down on a flat solid surface. Using a small head, 18 oz. ball peen hammer, fracture one face of the canister approximately 3/4" from the round edge, avoiding the exact center of the canister. Turn the canister over and repeat. Grab the bag by the edge and dispose of the canister and bag as UNCLASSIFIED trash.

A7.9.1. TO PUNCTURE: With a wide-blade screwdriver and hammer, puncture one flat side of the canister approximately 3/4" from the rounded edge, avoiding the exact center. Turn the canister over and repeat.

A7.9.2. TO SMASH: Place bagged canisters inside a canvas bag, or wrap loosely in a protective cloth, before smashing. Check to assure both flat sides are destroyed.

A7.10. Locally reproduce this instruction and provide a copy to each user issued key in canisters.

Attachment 8

IC 2003-1 TO AIR FORCE INSTRUCTION 33-211, COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS

31 OCTOBER 2003

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2003-1 (**Attachment 8**). Requires COMSEC managers to perform semiannual assessment and audits. Explains relief of accountability for the COMSEC Responsible Officer (CRO) and the users. Requires proof that the equipment is entered into the supply system before the material is issued to the CRO. Changes the requirement for keying material to be destroyed immediately after supersession instead of 12 hours after supersession. Requires exposed key tape segments be sealed in protective technology packaging or an opaque envelope. Deletes chopping as an approved method of destruction for COMSEC material. Adds new requirements for high security shredders and destruction methods of paper-mylar-paper key tapes. Provides more details on how to complete and retain Disposition Record Cards (DRC) with the local destruction report (SF-153). Changes retention of destruction certificates from 2 years to 3 years. Adds a Note about using another form of identification along with the Common Access Cards (CAC). Adds the Security Forces be notified in Task 2 of the Bomb Threat Task Cards.

3.1.9. Perform semiannual assessments and audits of the CRO according to AFI 33-230, Information Protection Assessment and Assistance Program (to become Information Assurance Assessment and Assistance Program) and AFKAG 2, Air Force COMSEC Accounting Manual.

3.3.21. Obtain relief of accountability from the COMSEC manager prior to leaving their current duty assignment. Ensure all COMSEC material is returned to the COMSEC manager and signed over to the new CRO.

3.4.6. Obtain relief of accountability from the CRO prior to being relieved of duties as a COMSEC user. The CRO must ensure users are not signed for any COMSEC material.

9.4. At a minimum the COMSEC records maintained by the CRO are operating instructions, emergency action plans, appointment letters, access list, requirements letter, AFCOMSEC Form 9, **Cryptographic Access Certificate (PA)**; AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**; AF Form 1109; **Visitor Register Log**; AFCOMSEC Form 16; AF Form 4168; DRC, destruction reports, hand receipts, waivers, EAP training, required reading, and semiannual assessments.

13.2. Process requests for most COMSEC equipment through the Standard Base Supply System (SBSS). Proof of accountability that the equipment has been entered into the SBSS is required before COMSEC managers issue keying material to CROs. Requests for space and EKMS related equipments (i.e., AN/CYZ-10, KGR-96) are processed through the COMSEC account. Send a COMSEC material requirements letter to the COMSEC manager at the same time to make sure COMSEC material is on hand when required. Direct questions to your supporting COMSEC manager.

16.2.2. When possible, issue keys electronically in a data transfer device (DTD). If physical key must be issued, issue key tape canisters in their entirety to include its associated disposition record card or appropriate form. Before issuing key canisters, the CRO will remove and destroy all superseded material. Air-

crew members must destroy any key tape segments removed from the canister immediately 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.

18.4. Verify personal clearance status from the currently approved security clearance verification roster, and that the person's need-to-know exists. CROs must review the authorized access list monthly to ensure its accuracy. Verify completion of the review by annotating the day, month, year and their initials on the list. Maintain only the most current access 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 forces office or other knowledgeable security offices.

21.10. On an AFCOMSEC Form 16, inventory classified and, or certified (e.g., KGR-96, KOK-13, etc.) 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. List DTDs on the inventory, regardless if keyed or unkeyed.

29.2. Destroy used keying material designated CRYPTO as soon as possible, but immediately after supersession. Under special circumstances (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.

29.2.2. Do not remove keytape segments stored in canisters until just before using or destroying them. Keep unused keytape segments in the keytape canister until needed or the canister's effective period ends. If you take out any keytape segments, destroy all superseded keytape segments immediately. Exposed key tape segments must be sealed in NSA protective technology packaging or an opaque envelope sealed in such a way that tampering would be obvious (i.e., writing the initial over the seal). Annotate the short title, ACN, segment, and quantity on the sealed envelope and store it with the canister and DRC. Use AFCOMSEC Form 21, AFCOMSEC Form 22A, AFCOMSEC Form 22B, or DRC 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 immediately 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 then destroy it immediately after supersession. Document unreliable circuits to the controlling authority with a letter, e-mail, or message and annotate the authority on the DRC. (3) Disposition records used for unclassified ALC-1, ALC-6, or ALC-7 keying material are UNCLASSIFIED FOR OFFICIAL USE ONLY when filled in.

29.2.2.1. When making annotations on the disposition record (e.g., AFCOMSEC Form 22B, DRC, etc.), individuals will place date, signature or initial, in each applicable block. For Top Secret keytapes two initials are required for issue to validate that TPI procedures are being followed.

29.2.2.1.1. For partial canisters: If segments 1 through 10 are used within a canister and segments 11 through 31 remain at the end of the month and must be destroyed, the remainder of the canister may be “Z”d on the DRC.

29.2.2.1.2. For entire canisters:

29.2.2.1.2.1. If no segments were issued, destroy the entire canister, complete an SF-153 only, annotate after the "Nothing Follows" – "No segments issued" and both the destruction official and witness will initial next to the statement. No DRC is required.

29.2.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement. No DRC is required.

29.2.2.1.2.3. If all segments are loaded into a DTD and the segments need to be retained, (circuit must be unreliable and you must have something from the controlling authority stating to retain keying material) seal the segments in NSA protective packaging or an opaque envelope where tampering is evident. Superseded key must be destroyed during the month if the material locked in a safe is accessed during the month. Annotate the DRC the same as partial canisters.

29.6. Destroy compromised material immediately after you receive disposition instructions or upon receipt of case closure from AFCA.

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

30.1.2. When pulping or pulverizing paper COMSEC aids, break the material into bits no larger than five millimeters.

30.1.3. Key tapes are paper-mylar-paper. The only approved methods for destroying key tapes are by a disintegrator, burning, or pulverizing. Do not place keying material in burn bags for destruction along with other classified waste.

30.2. 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 melting, pulverizing, and chemical alteration.

32.1.1. Use the DRC provided to record destruction of each key setting. Destroy unused key, pages, tables, or day sheet, etc., when you load a current one or immediately after supersession.

32.1.2. Provide a copy of all completed destruction records (SF 153) to the COMSEC account no later than the first duty day after the material supersession. The CRO will attach the completed DRCs to the applicable SF 153. These may be maintained by the CRO or the COMSEC account; it is the COMSEC Manager's choice. When the DRCs are attached the SF 153 becomes CONFIDENTIAL.

32.1.4. For items issued to transient or deploying aircrews not returning to your location, file a copy of the signed, annotated receipt and keep it for 3 years after the yearly cutoff. Returning aircrews must immediately give unused material and DRC to their CRO.

32.2.2. When the COMSEC manager directs, destroy the material, record destruction of classified documents on a SF 153, and keep the destruction certificate for 3 years according to AFMAN 37-139.

59.2. Users positively identify all COMSEC assessors by comparing the identification card (DD Form 2, **Armed Forces Identification Card [Active, Reserve, and Retired]**, Common Access Card, or Air Force Form 354, **Civilian Identification Card**) with the assessment/audit message notice, TDY orders, or records the COMSEC manager provides. Sign them in on the Air Force Form 1109 or FAA Form 1600-8 (for FAA accounts). ***NOTE:*** Another form of ID may be needed with the CAC since SSNs are not

listed on civilian or contractor CACs. Use a valid state driver license or a recent payroll statement as a second form of ID with the CAC.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 104-13, *The Paperwork Reduction Act of 1995*

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

AFPD 33-2, *Information Protection*

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

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 33-201, *Communications Security (COMSEC) (FOUO)*

AFI 33-210, *Cryptographic Access Program*

AFI 33-212, *Reporting COMSEC Deviations*

AFI 33-230, *Information Protection Assessment and Assistance Program (*will become *Information Assurance Assessment and Assistance Program)*

AFI 33-275, *Controlled Cryptographic Items*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFMAN 23-110, *USAF Supply Manual*

AFMAN 33-272, (S) *Classifying COMSEC and TEMPEST Information* (U) (will become *Classifying Information Assurance Information (U)*)

AFMAN 37-139, *Records Disposition Schedule*

AFDIR 33-303, *Compendium of Communications and Information Technolog*y

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

AFKAG-2, *Air Force COMSEC Accounting Manual*

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

Abbreviations and Acronyms

ACN Accounting Control Number

AFCA Air Force Communications Agency

AFCOMSEC Air Force Communications Security

AFI Air Force Instruction

AFMAN Air Force Manual

AFPD Air Force Policy Directive

AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Manual
ALC	Accounting Legend Code
CAP	Cryptographic Access Program
CCI	Controlled Cryptographic Item
CIK	Crypto-Ignition Key
CJCSI	Chairman of the Joint Chief of Staff Instruction
CMCS	COMSEC Material Control System
CM^2	Computerized Management of COMSEC Material
CNLZ	COMSEC No-Lone Zone
COMSEC	Communications Security
CONUS	Continental United States
COR	Central Office of Record
CRO	COMSEC Responsible Officer
DRC	Disposition Record Card
DRU	Direct Reporting Unit
DTD	Data Transfer Device
EAP	Emergency Action Plan
EKMS	Electronic Key Management System
EOM	End of Month
FAA	Federal Aviation Administration
FOA	Field Operating Agency
GS	General Schedule
GSA	General Services Administration
IAAP	Information Assurance Assessment and Assistance Program
MAJCOM	Major Command
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OI	Operating Instruction
PAL	Permissive Action Link
PROM	Programmable Read-Only Memory
RON	Remain Overnight

SAS Sealed Authenticator System

SBSS Standard Base Supply System

SCI Sensitive Compartmented Information

SCIF Sensitive Compartmented Information Facility

SF Standard Form

SSN Social Security Account Number

STU Secure Telephone Unit

TDY Temporary Duty

TPI Two-Person Integrity

UCM[2] Users Computerized Management of COMSEC Material

URL Uniform Resource Locator

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, and so forth, marked CRYPTO), call sign 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.

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 (COR), 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.

Electronic Key Management System (EKMS) Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generation, distribut-

ing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

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 (for example: "HQ AFCA requires material in support of Operation Plan (OPLAN), JCS Exercise_____, and so forth" General statements, such as "to fulfill mission requirements" or "as directed by XYZ message 091234Z Jan 02," are not accepted by themselves; we need further justification.)

3. Attached is proof that the equipment has been entered into the Standard Base Supply System according to AFMAN 23-110.

(*Signature Element of CRO*)

Attachment 5

SAMPLE -- COMMUNICATIONS SECURITY EMERGENCY ACTION PLAN

A5.1. Fire Task Cards.

EXAMPLE - Task Card #1:

-- Purpose. Provides for orderly evacuation of personnel and protection of COMSEC material within facilities using COMSEC aids and equipment in case of fire.

-- The senior person present implements the plan by issuing task cards. If a limited number of personnel are available to carry out each task, combine the tasks.

-- After the fire is out, inspect the safes for signs of entry or tampering and take a complete inventory of all COMSEC material.

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

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

EXAMPLE - Task Card #2.

-- Sound alarm and notify Fire Department, stating: **THIS IS** (*Rank/Name*)**, REPORTING A FIRE IN BUILDING _____, ROOM _____.**

-- Do not hang up the telephone until the fire dispatcher knows the location and has no questions.

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

EXAMPLE - Task Card #3.

-- Secure all COMSEC material (keytapes, keylists, code books, Data Transfer Device (DTD), and so forth), the STU-III keys, and all other classified material in the safe along with COMSEC inventories.

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

EXAMPLE - Task Card #4.

-- Fight any open fire, if possible, using available fire extinguishers.

-- Fire extinguisher(s) (*Type*) is/are located _____(*where*)_____.

EXAMPLE - Task Card #5.

-- Open and guard the door that gives fire department personnel greatest access to the fire.

-- Admit all firefighting personnel, including local national firefighters.

EXAMPLE - Task Card #6.

-- Notify the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- Manager, COMSEC account _____ (duty hour phone number _____ and non-duty hour phone number _____).

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

EXAMPLE - Task Card #7.

-- Take names of all Fire Fighters for inadvertent oath, if necessary.

-- Take inventory to ensure all material is present.

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

A5.2. Natural Disaster Task Cards:

EXAMPLE - Task Card #1.

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

-- 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 are available to carry out the tasks, combine the tasks.

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

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

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

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

EXAMPLE - Task Card #3.

-- If time and circumstances permit, destroy all superseded COMSEC material and annotate the destruction.

EXAMPLE - Task Card #4.

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

A5.3. Bomb Threat Task Cards:

EXAMPLE - Task Card #1.

-- Purpose. To protect COMSEC material in facilities using COMSEC materials in the event of a bomb threat.

-- 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 are available to carry out the tasks, combine the tasks.

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

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

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

EXAMPLE - Task Card #2.

-- Notify the Security Forces.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

EXAMPLE - Task Card #3.

-- Gather and secure all COMSEC material (keytapes, keylists, code books, DTD, etc.), the STU-III keys, and classified material in the safe along with the COMSEC inventories.

-- Leave the building and go to the designated assembly point located (enter location).

EXAMPLE - Task Card #4.

-- Conduct a search of the area and look for suspicious objects.

-- If found, guard the entrance and admit only authorized personnel until security police take over.

-- If not found, leave the building and go to the designated assembly point located (enter location).

A5.4. Emergency Evacuation Task Cards:

EXAMPLE - Task Card #1.

-- Purpose. To protect COMSEC material in facilities using COMSEC aids and equipment during emergency evacuation.

-- 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 are available to carry out the tasks, combine the tasks.

-- After the emergency, completely inventory all COMSEC material.

-- If you suspect tampering or damage, thoroughly page check all COMSEC items.

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

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

EXAMPLE - Task Card #3.

-- If time permits, destroy all superseded COMSEC aids.

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

EXAMPLE - Task Card #4.

-- Gather all current material required for immediate secure communications, as well as the COMSEC inventory, and put them in a canvas bag.

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

EXAMPLE - Task Card #5.

-- Remove COMSEC aids in use from all COMSEC equipment and put them in a canvas bag.

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

EXAMPLE - Task Card #6.

-- Secure the facility as well as possible so forced entry will be obvious.

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

EXAMPLE - Task Card #7.

-- If you expect to evacuate for a short time, secure all other COMSEC items (including future COMSEC aids) in an approved storage container.

-- Put material required to maintain secure communications in a canvas bag.

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

EXAMPLE - Task Card #8.

-- Evacuate the material, under constant surveillance, preferably by authorized personnel, to the designated evacuation site and begin secure communications.

A5.5. Emergency Destruction Task Cards

A5.5.1. Phase I--Precautionary Destruction Task Cards:

EXAMPLE - Task Card #1.

-- Purpose: To provide guidelines for:

--- Destroying COMSEC material during emergencies resulting from natural, accidental, or hostile causes.

--- Reducing holdings as a precautionary measure.

--- Preventing their capture or compromise in an actual emergency or attack.

-- Personnel authorized to implement this plan:

--- Commander (applicable unit).

--- Commander (issuing COMSEC account unit).

--- Manager, COMSEC account.

--- CRO or alternate.

--- Senior member present.

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

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

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

EXAMPLE - Task Card #3.

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

-- 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.

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

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

EXAMPLE - Task Card #4.

-- Go to the incinerator in Building _____ and fire it up.

-- The material for destruction is brought to you.

-- Place it in the incinerator as you receive it.

-- Tend the incinerator until all material is burned.

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

EXAMPLE - Task Card #5.

-- Gather all superseded COMSEC aids, using the attached Priority of Destruction list, and place in canvas bags.

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #6.

-- Gather all future COMSEC aids (those not scheduled to go into effect within the next 60 days), using the destruction priority listing, and place in canvas bags.

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #7.

-- Gather all administrative documents, files, training aids, and other material not required for continued operations and place in canvas bags.

-- Take the bags to the incinerator for destruction.

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

A5.5.2. Phase II--Total Emergency Destruction Task Cards:

EXAMPLE - Task Card #1.

-- Purpose: To provide guidance for preventing capture or compromise of COMSEC material in an actual emergency or attack.

-- 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.

-- After emergency destruction or as soon as possible if emergency destruction is not completed, record all destruction on the preaddressed emergency destruction letter and carry it to the COMSEC manager.

EXAMPLE - Task Card #2.

-- Notify the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

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

EXAMPLE - Task Card #3.

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

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

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

EXAMPLE - Task Card #4.

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

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

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

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

EXAMPLE - Task Card #5.

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

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

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #6.

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

-- Take the bags to the incinerator for destruction.

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

EXAMPLE - Task Card #7.

-- Remove all classified and Controlled Cryptographic Item (CCI) boards from the COMSEC equipment, thoroughly smash them with a hammer or an ax, and scatter the pieces.

-- Document destruction on the COMSEC inventory (AFCOMSEC Form 16).

-- Write names of unlisted items on the back of the form.

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

A5.6. 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.

A5.6.1. Keying Material.

A5.6.1.1. All superseded keying material and future editions of sealed authenticator system (SAS) and permissive action list (PAL) material:

A5.6.1.1.1. TOP SECRET (shared material ahead of point-to-point).

A5.6.1.1.2. SECRET (shared material ahead of point-to-point).

A5.6.1.1.3. CONFIDENTIAL (shared information ahead of point-to-point).

A5.6.1.2. All current keying material (zeroize all cryptographic equipment and remove and destroy current keylists and keytapes).

A5.6.1.2.1. TOP SECRET (shared information ahead of point-to-point).

A5.6.1.2.2. SECRET (shared information ahead of point-to-point).

A5.6.1.2.3. CONFIDENTIAL (shared information ahead of point-to-point).

A5.6.1.3. All future keylists, keytapes, codes, and authenticators scheduled to take effect within the next 30 days:

A5.6.1.3.1. TOP SECRET (shared information).

A5.6.1.3.2. SECRET (shared information).

A5.6.1.3.3. CONFIDENTIAL (shared information).

A5.6.1.4. All remaining future keying material.

A5.6.2. COMSEC Documents.

A5.6.2.1. Sensitive pages of cryptographic equipment maintenance manuals.

A5.6.2.2. Remaining classified documents.

A5.6.2.3. Classified COMSEC files.

A5.6.3. Cryptographic Equipment.

A5.6.3.1. Remove and destroy (time permitting), and list location.

A5.6.3.1.1. Readily removable classified and sensitive CCI elements.

A5.6.3.1.2. Remaining classified and sensitive CCI parts or components.

Attachment 7

HANDLING INSTRUCTIONS FOR ALL KEYTAPES

A7.1. Do not remove keytape segments until immediately prior to use or destruction. DO NOT REMOVE TAPE SEGMENTS FOR INVENTORY. If a tactical user requires more key than can be set or electrically stored in the crypto-equipment, the user may furnish additional key in electrical form in a common fill device or in hard copy form in a tape canister. Do not issue tape segments as extracts.

A7.2. Maintain the applicable disposition record card (DRC) for each keytape canister. Retain completed DRC and attach it to the local destruction report (SF 153).

A7.2.1. When making annotations on the disposition record (e.g., AFCOMSEC Form 22B, DRC, etc.), individuals will place date, signature or initial, in each applicable block. For Top Secret keytapes two initials are required for issue to validate that TPI procedures are being followed.

A7.2.1.1. For partial canisters: If segments 1 through 10 are used within a canister and segments 11 through 31 remain at the end of the month and must be destroyed, the remainder of the canister may be "Z"d on the DRC.

A7.2.1.2. For entire canisters:

A7.2.1.2.1. If no segments were issued, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" – "No segments issued" and both the destruction official and witness will initial next to the statement. No DRC is required.

A7.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement. No DRC is required.

A7.2.1.2.3. If all segments are loaded into a DTD and the segments need to be retained, (circuit must be unreliable and you must have something from the controlling authority stating to retain keying material)

seal the segments in NSA protective packaging or an opaque envelope where tampering is evident. Superseded key must be destroyed during the month if the material locked in a safe is accessed during the month. Annotate the DRC the same as partial canisters.

A7.3. COMSEC managers may destroy segments of unissued tapes as they are superseded or may destroy unissued tapes as whole editions.

A7.4. Some key that is designated for off-the-air use (e.g., maintenance, test, classroom training, and demonstrations) has no prescribed cryptoperiod and may be used until no longer serviceable and then destroyed.

A7.5. Reproduction of associated tape is prohibited without the approval of the controlling authority.

A7.6. Notify the controlling authority immediately if the associated tape is lost, subjected to unauthorized viewing, or possibly compromised in any way. Report any incident according to AFI 33-212.

A7.7. Canister Disposition Instructions: Remove barcode stickers and destroy as classified trash. Once the key has been superseded and removed from the canister, destroy both large flat surfaces of the canister. The destruction of the canister requires that you follow the DESTRUCTION PROCEDURE below, and in addition, apply the proper SAFETY PROCEDURES at the time of destruction.

A7.8. Safety Procedures. An empty tape canister will shatter if fractured with a blunt instrument. To protect from possible injury due to flying fragments, place the canister inside a zip-lock plastic bag or similar sealable bag before beginning the destruction procedure. Wear protective eyewear during the destruction procedure to prevent injury.

A7.9. Destruction Procedure. Place the canister inside a zip-lock plastic bag or similar sealable bag, and set it down on a flat solid surface. Using a small head, 18 oz. ball peen hammer, fracture one face of the canister approximately 3/4" from the round edge, avoiding the exact center of the canister. Turn the canister over and repeat. Grab the bag by the edge and dispose of the canister and bag as UNCLASSIFIED trash.

A7.9.1. TO PUNCTURE: With a wide-blade screwdriver and hammer, puncture one flat side of the canister approximately 3/4" from the rounded edge, avoiding the exact center. Turn the canister over and repeat.

A7.9.2. TO SMASH: Place bagged canisters inside a canvas bag, or wrap loosely in a protective cloth, before smashing. Check to assure both flat sides are destroyed.

A7.10. Locally reproduce this instruction and provide a copy to each user issued key in canisters.

Attachment 9

IC 2004-1 TO AIR FORCE INSTRUCTION 33-211, COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS

3 JUNE 2004

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*); AFI 33-201, *Communications Security (COMSEC)(FOUO)*; 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 issues to them. This instruction applies to all Air Force military, civilian, and contractor personnel under contract by the Department of Defense (DoD) who handle COMSEC materials. This instruction takes precedence over all conflicting Air Force documents. Additional instructions and manuals are listed on the Air Force Publishing Web site at Uniform Resource Locator (URL): **http://www.e-publishing.af.mil** under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/WFP, and Headquarters United States Air Force (HQ USAF/XICI), 1800 Air Force Pentagon, Washington DC 20330-1800. Major commands (MAJCOM), field operating agencies (FOA), and direct reporting units (DRU) send one copy of final supplement to HQ AFCA/WFP and HQ AFCA/ITXD. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force Web-RIMS *Records Disposition Schedule (RDS)* located at **https://webrims.amc.af.mil/rds/index.cfm**. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*, affect this publication. See **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2004-1. The update provides references to specific instructions for the handling of NATO, NATO Nuclear Command and Control COMSEC materials, and positive control materials. The change requires the COMSEC manager to coordinate on all requests for new COMSEC equipment. It requires training for all personnel on the access lists and deletes the CRO and alternate CRO from training. This change adds procedures to establish material distribution if unit is deployed more than 6 months. This update deletes the usage of AFCOMSEC Forms 21, 22A, and 22B and establishes use of the disposition record cards only. The update changes the CIK of a DTD that holds SCI keying material to be stored in under TPI controls. This update provides additional information about the software program, Users Computerized Management of COMSEC Material (UCM^2). This change deletes the requirement to use “red ink” and “green ink” to “a specific color” on changes made to inven-

tories. It adds instructions on who can sign appointment letters for contractors, and allows them to use a company form for visitor entry instead of an AF Form 1109. This update adds that the COMSEC manager provides the CRO with after duty hours notification contact numbers. It also adds that the COMSEC operational and maintenance manuals will be maintained for the equipment held by the user. The change adds instructions that the destruction and witnessing officials be physically present and that they never sign the destruction form in advance when destroying material.

1.1. Safeguard and control NATO Nuclear Command and Control COMSEC Material as described in AMSG-773, *Policy and Procedures for Handling and Control of Two-Person Controlled (TPC) NATO Sealed Authentication System (SAS)*.

1.2. Safeguard and control other NATO material as prescribed in AMSG-293, *NATO Cryptographic Instruction*.

1.3. Safeguard and control Joint Staff positive control material and devices (i.e., Sealed Authenticator System, Permissive Action Link, Coded Switch System, Positive Enable System, and Nuclear Certified Computer Data) as prescribed in Chairman Joint Chiefs of Staff Instruction (CJCSI) 3260.01, *Policy Governing Positive Control Material*.

3.1.10. Coordinate on AF Form 3215, **C4 Systems Requirement Document**, identifying COMSEC equipment requirements, and order COMSEC devices that are in COMSEC Material Control System (CMCS) according to AFKAG 2.

3.1.11. Provide a contact number for non-duty notification to the CRO and users to report all known or suspected COMSEC deviations.

3.3.3 Make sure all persons granted access to COMSEC materials have a final security clearance equal to or greater than the classification level of the COMSEC material to be accessed and have a valid need-to-know.

3.3.19. All personnel granted access to COMSEC must be familiar with applicable Air Force and specialized COMSEC publications (e.g., OIs, AFI 33-211, AFSSIs, KAMs, KAOs, etc.). These personnel must maintain this familiarization by accomplishing semiannual training. To validate this training all personnel will sign and date the review documentation developed by the CRO. Personnel on leave or temporary duty (TDY) must complete this training upon return to duty section.

3.3.22. Obtain new COMSEC equipment according to AFI 33-103, *Requirements Development and Processing*. Coordinate with the COMSEC manager on all requirements.

3.4.3. Maintain and familiarize themselves with correct procedures for operating associated cryptographic equipment and devices utilizing applicable AFSSIs, AFKAOs, KAOs, or instructions provided by the CRO.

4. Appointing COMSEC Responsible Officers (CRO). Unit commanders (or equivalents, Facility Security Officer for contractors) appoint, 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 materials to and from. Update this letter at least annually or as changes occur.

5. Training. CROs use this AFI and other applicable publications to set up a comprehensive, periodic training program for COMSEC Users. Training is mandatory for all personnel listed on the access list.

Ensure all personnel with authorized access know how to handle, control, and use the COMSEC material. Ensure that all personnel are familiar with correct procedures in operating associated cryptographic equipment utilizing applicable AFKAOs, KAOs, AFSSIs, or similar instruction provided by the COMSEC manager. Use AF Form 4168, **COMSEC Responsible Officer and User Training Checklist,** to document initial and refresher training of all users. Complete a separate training checklist for each person with access. Each block beside each item that applies must contain the initials of the trainer and trainee. Provide annual refresher training to all personnel who have been granted access. Accomplish training at least every 365 days. Document annual training by completing a new AF Form 4168. Maintain only the most current form on file.

6. Operating Instructions (OI). Each CRO must write COMSEC OIs and coordinate them with the COMSEC manager for review and endorsement prior to its implementation. The OIs contain provisions for securely conducting COMSEC operations (in both normal and emergency situations) and for safeguarding COMSEC material. The procedures and instructions in the OIs are specific to the user's activity. A contractor CRO may title its operating instructions as Standard Practice Procedure or by another other corporate nomenclature as long as it meets the requirements set by this instruction.

6.3. Units with a deployable mission will develop procedures on handling, controlling, and protecting COMSEC materials while deployed. Ensure these procedures are established in a separate OI for use when deployed, and it is marked or annotated to indicate clearly it is to be used only when on deployment. Maintain it separately from the in-garrison OI to avoid potential confusion.

9.2.1. Limit access to these records and files to those persons who manage, administer, operate, and maintain COMSEC aids and equipment. MAJCOM approval is required if outside agencies such as the Air Force Audit Agency or Inspector General require viewing of COMSEC documentation.

9.5. User Computerized Management of COMSEC Material (UCM^2) is the Air Force software program used to manage COMSEC material at the User account level. It consists of a computer database designed to assist COMSEC CROs in their daily accounting activity. UCM^2 facilitates the tedious day-to-day accounting, decreases accounting discrepancies, and reduces the required paperwork that audits COMSEC accounting transactions. UCM^2 must be loaded onto a standalone computer. UCM^2 becomes classified SECRET if the effective dates of COMSEC materials are entered. Do **NOT** enter UCM^2 onto the Secret Internet Protocol Router Network (SIPRNET).

10.4. ALC-6 is electronically generated key that is continuously accountable to the Central Office of Record (COR) by means of EKMS elements. Tier 0 or Tier 1 within the EKMS system generates the electronic key. Account for keys on hand receipts and local DRCs.

10.5. ALC-7 is electronically generated keying material that is continuously accountable locally within EKMS elements. Keys are generated locally by the COMSEC account. Account for keys on hand receipts and local disposition records (e.g., DRC, MAJCOM approved form, etc.).

12. Disposition Record Cards. The COMSEC manager enters the required status information on the Disposition Record Cards (created by the CRO using UCM^2) or on the front covers before issuing COMSEC aids. When material is issued, date and initial each block individually.

13.1. CROs must review and validate their unit's COMSEC requirements (Key and Equipment) annually. After the review and validation, the CRO must provide the COMSEC manager a written list of all COMSEC requirements to include the justification (i.e., plan, regulation, operation order) for each item. If

equipment is required ensure the associated instructions (KAO, KAM, etc.) issued by the COMSEC account is included.

14.1. Deploying units must take current plus 90 days of material with them. If there is a local COMSEC account to support them, turn the material over to the account, setup monthly distribution and follow their instructions. Distribution should only be changed if the unit will be deployed longer than 6 months.

16.2.1. Page check and seal documents (i.e., code books, authenticators, etc.). Seal documents by using a **white address label (or similar label) around one of the nonbound ends (right side, top or bottom). Initials would then be written over the label and on to the document to detect tampering or usage**. Issue the sealed document and disposition record card 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 immediately after supersession and annotate this destruction on the DRC provided destruction facilities are available. If destruction facilities are not available, hold material until the aircrew arrives at a location where destruction facilities are available.

16.3.1. Aircrews may carry complete canisters of keytapes or keylists (current plus 3 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 immediately after supersession provided destruction facilities are available. If destruction facilities are not available, hold the superseded material until the aircrew arrives at a location where destruction facilities are available.

16.5.4. Lock the aircraft and the container. If the aircraft is not lockable, then seal the doors. US personnel must check the aircraft and container the first duty hour after crew rest for signs of tampering or penetration. Report any suspected tampering according to AFI 33-212.

16.6. Handling and Controlling of Sensitive Compartmented Information (SCI) Keying Material. Any segment pulled from its canister and loaded for encryption must be treated as SCI and destroyed immediately inside a Sensitive Compartmented Information Facility (SCIF). Store segments remaining inside the canister within a SCIF. Whenever possible, use electronic key rather than paper tapes. Retention of used paper tape key segments is not recommended unless the exposed key segments are retained in NSA protected packaging. Key segments inside a canister that have never been used and become superseded must be pulled for destruction while in a SCIF. DTDs loaded with SCI keying material must be stored in a SCIF, in an approved Top Secret safe separate from the CIK. The CIK must be stored under Two Person Integrity (TPI). Load SCI keying material segments into a KYK-13 while in a SCIF and destroy the exposed segment immediately.

18.3. Limit 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, rank, full SSN, and clearance levels of all persons who have COMSEC responsibilities in the facility, and may include the unit commander and supervisors. All personnel on the list must have a final security clearance equal to or higher than the COMSEC information to which they have access. All personnel listed on the access list must have completed COMSEC training before being allowed access to the COMSEC material. Refer to AFI 31-501, *Personnel Security Program Management*, for processing of security clearances.

18.4. Verify personal clearance status from the currently approved security clearance verification roster, and that the person's need-to-know exists. CROs must review the authorized access list monthly to ensure its accuracy and then annotate the review date, month, and their initials on the list. Maintain only the most

current access list. ***NOTE:*** The authorizing official (for FAA, Facility Manager; for contractors, Facility Security Officer) or CRO signs the authorized access list. Get security clearance information for civilian personnel (including DoD and civil agency contractors) from the base security forces office or other knowledgeable security offices.

18.6. Record the arrival and departure of all persons not named on the authorized access list, using AF Form 1109, Federal Aviation Administration (FAA) Form 1600-8 (for FAA use only), or a local company form (for CRO contractors with COMSEC managers approval). For COMSEC users in controlled areas, keep an additional separate visitor register to record access to COMSEC material. Retain the AF Form 1109, FAA Form 1600-8 (for FAA use only), or company form on file for 1 year after date of last visitor recorded on the form.

21.4.2. Use a specific color when removing an item from the AFCOMSEC Form 16. Block out the remainder of that entry, date, initial, and explain the reason for removal (e.g., Returned to account, Destroyed voucher number ##, etc.) When deleting a single item from a multiple line entry, completely remove the item from the inventory and readd the remaining items to the end of the inventory as a new entry.

21.4.3. Use a specific color when adding items to the AFCOMSEC Form 16. Block the entry up to the date added, date, initial, and explain the reason for the addition (e.g., Received from account, etc.) If a new inventory is printed out, identify items added on the new inventory.

21.5.3. 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 1 day. Provide inventories to the CRO upon mission completion. File these inventories with the other inventories for the month and retain for 6 months.

29.2. Destroy used keying material designated CRYPTO as soon as possible, but immediately after supersession. See applicable AFSSI for key reuse and holding rules. Under special circumstances (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.

29.2.2. Do not remove keytape segments stored in canisters until just before using or destroying them. Keep unused keytape segments in the keytape canister until needed or the canister's effective period ends. If you take out any keytape segments, destroy all superseded keytape segments immediately. Exposed key tape segments must be sealed in NSA protective technology packaging or an opaque envelope sealed in such a way that tampering would be obvious (i.e., writing the signatures/initials over the seal). If material is TPI, two sets of signatures/initials are required. Annotate on the short title, ACN, segment, and quantity on the sealed envelope and store it with the canister and DRC. Use DRC 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 immediately 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 then destroy it immediately after supersession. Document unreliable circuits to the controlling authority with a letter, e-mail, or message and annotate the authority on the DRC. (3) Disposition records used for unclassified ALC-1, ALC-6, or ALC-7 keying material are UNCLASSIFIED FOR OFFICIAL USE ONLY when filled in.

29.2.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, complete an SF-153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement.

31.1. The destruction official is an appropriately cleared, responsible individual. The destruction official will be physically present and perform the destruction of the material listed in the destruction report. ***NOTE:*** Since there is no formal grade requirement, CROs must ensure officials are trustworthy and knowledgeable.

31.2. The witnessing official must have a clearance consistent with the material being destroyed. The witnessing official will be physically present and view the destruction of the material listed in the destruction report. 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.

31.3. Sign the destruction report by the destruction official and the witnessing official once the destruction is complete and they have checked the destruction machine and area for residue. Destruction reports will never be signed in advance of the actual destruction by either the destruction or witnessing official. Ensure all destruction requirements set by this instruction are met before signing the destruction report.

61.5. **DELETED.**

61.6. **DELETED.**

61.7. The COMSEC manager closes open items on the assessment report once the corrective action has been completed.

61.8. Keep all assessment/audit reports on file from one command assessment to the next command assessment.

61.9. If a user is rated Unsatisfactory, the wing COMSEC manager notifies the CRO's commander in person and conducts another assessment/audit within 90 days.

62.2. Records: Maintain and dispose of records created by this publication according to Air Force Web-RIMS RDS, Table 33-22, Rules 1, 2.01, 2.02, 3, 5, 5.01, 6, 8, 9, and 26, located at **https://webrims.amc.af.mil/rds/index.cfm**.

62.3.1. Adopted Forms: SF 153, **COMSEC Material Report**; SF 700, **Security Container Information**; SF 701, **Activity Security Checklist**; SF 702, **Security Container Check Sheet**; DD Form 2, **Armed Forces Identification Card (Active, Reserve, and Retired)**; DD Form 254, **DOD Contract Security Classification Specification**; DD Form 1753, **Master Station Log**; AF Form 12, **Accountable Container Receipt**; AF Form 354, **Civilian Identification Card**; AF Form 847, **Recommendation for Change of Publication**; AF 1109, **Visitor Register Log**; AF Form 3215, **C4 Systems Requirement Document**; AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria;** AF Form 4168, **COMSEC Responsible Officer and User Training Checklist;** AFCOMSEC Form 9, **Cryptographic Access Certificate (PA)**; AFCOMSEC Form 16, **COMSEC Account Daily - Shift Inventory**; and AFTO Form 36, **Maintenance Record for Security Type Equipment.**

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 104-13, *The Paperwork Reduction Act of 1995*

AMSG-293, *NATO Cryptographic Instruction*

AMSG-773, *Policy and Procedures for Handling and Control of Two-Person Controlled (TPC) NATO Sealed Authentication System (SAS)*

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

CJCSI 3260.01, *Policy Governing Positive Control Material*

AFPD 33-2, *Information Protection (*will become *Information Assurance)*

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

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-210, *Cryptographic Access Program*

AFI 33-212, *Reporting COMSEC Deviations*

AFI 33-230, *Information Protection Assessment and Assistance Program (*will become *Information Assurance Assessment and Assistance Program)*

AFI 33-275, *Controlled Cryptographic Items*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFMAN 23-110, *USAF Supply Manual*

AFMAN 33-272, (S) *Classifying COMSEC and TEMPEST Information* (U) (will become *Classifying Information Assurance Information (U)*)

AFMAN 37-123, *Management of Records*

AFMAN 37-139, DELETED

AFDIR 33-303, *Compendium of Communications and Information Technolog*y

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

AFKAG-2, *Air Force COMSEC Accounting Manual*

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

Web-RIMS, *Records Disposition Schedule (RDS)*

Abbreviations and Acronyms

ACN	Accounting Control Number
AFCA	Air Force Communications Agency
AFCOMSEC	Air Force Communications Security
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFPD	Air Force Policy Directive
AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Manual
ALC	Accounting Legend Code
CAP	Cryptographic Access Program
CCI	Controlled Cryptographic Item
CIK	Crypto-Ignition Key
CJCSI	Chairman of the Joint Chief of Staff Instruction
CMCS	COMSEC Material Control System
CM^2	Computerized Management of COMSEC Material
CNLZ	COMSEC No-Lone Zone
COMSEC	Communications Security
CONUS	Continental United States
COR	Central Office of Record
CRO	COMSEC Responsible Officer
DRC	Disposition Record Card
DRU	Direct Reporting Unit
DTD	Data Transfer Device
EAP	Emergency Action Plan
EKMS	Electronic Key Management System
EOM	End of Month
FAA	Federal Aviation Administration
FOA	Field Operating Agency
GS	General Schedule
GSA	General Services Administration
IAAP	Information Assurance Assessment and Assistance Program

MAJCOM	Major Command
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OI	Operating Instruction
PAL	Permissive Action Link
PROM	Programmable Read-Only Memory
RDS	Records Disposition Schedule
RON	Remain Overnight
SAS	Sealed Authenticator System
SBSS	Standard Base Supply System
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SF	Standard Form
SSN	Social Security Number
STU	Secure Telephone Unit
TDY	Temporary Duty
TPI	Two-Person Integrity
UCM^2	Users Computerized Management of COMSEC Material
URL	Uniform Resource Locator

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, and so forth, marked CRYPTO), call sign 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.

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 (COR), 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.

Electronic Key Management System (EKMS). Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generation, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

Attachment 7

HANDLING INSTRUCTIONS FOR ALL KEYTAPES

A7.1. Do not remove keytape segments until immediately prior to use or destruction. DO NOT REMOVE TAPE SEGMENTS FOR INVENTORY. If a tactical user requires more key than can be set or electrically stored in the crypto-equipment, the user may furnish additional key in electrical form in a common fill device or in hard copy form in a tape canister. Do not issue tape segments as extracts.

A7.2. Maintain the applicable disposition record card (DRC) for each keytape canister. Retain completed DRC and attach it to the local destruction report (SF 153).

A7.2.1. When making annotations on the DRCs, individuals will place date, signature or initial, in each applicable block. For Top Secret keytapes two initials are required for issue to validate that TPI procedures are being followed.

A7.2.1.1. <u>For partial canisters</u>: If segments 1 through 10 are used within a canister and segments 11 through 31 remain at the end of the month and must be destroyed, the remainder of the canister may be "Z"d on the DRC.

A7.2.1.2. <u>For entire canisters:</u>

A7.2.1.2.1. If no segments were issued, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" – "No segments issued" and both the destruction official and witness will initial next to the statement. No DRC is required.

A7.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement. No DRC is required.

A7.2.1.2.3. If all segments are loaded into a DTD and the segments need to be retained, (circuit must be unreliable and you must have something from the controlling authority stating to retain keying material) seal the segments in NSA protective packaging or an opaque envelope where tampering is evident. Superseded key must be destroyed during the month if the material locked in a safe is accessed during the month. Annotate the DRC the same as partial canisters.

A7.3. COMSEC managers may destroy segments of unissued tapes as they are superseded or may destroy unissued tapes as whole editions.

A7.4. Some key that is designated for off-the-air use (e.g., maintenance, test, classroom training, and demonstrations) has no prescribed cryptoperiod and may be used until no longer serviceable and then destroyed.

A7.5. Reproduction of associated tape is prohibited without the approval of the controlling authority.

A7.6. Notify the controlling authority immediately if the associated tape is lost, subjected to unauthorized viewing, or possibly compromised in any way. Report any incident according to AFI 33-212.

A7.7. Canister Disposition Instructions: Remove barcode stickers and destroy as classified trash. Once the key has been superseded and removed from the canister, destroy both large flat surfaces of the canister. The destruction of the canister requires that you follow the DESTRUCTION PROCEDURE below, and in addition, apply the proper SAFETY PROCEDURES at the time of destruction.

A7.8. Safety Procedures. An empty tape canister will shatter if fractured with a blunt instrument. To protect from possible injury due to flying fragments, place the canister inside a zip-lock plastic bag or similar sealable bag before beginning the destruction procedure. Wear protective eyewear during the destruction procedure to prevent injury.

A7.9. Destruction Procedure. Place the canister inside a zip-lock plastic bag or similar sealable bag, and set it down on a flat solid surface. Using a small head, 18 oz. ball peen hammer, fracture one face of the canister approximately 3/4" from the round edge, avoiding the exact center of the canister. Turn the canister over and repeat. Grab the bag by the edge and dispose of the canister and bag as UNCLASSIFIED trash.

A7.9.1. TO PUNCTURE: With a wide-blade screwdriver and hammer, puncture one flat side of the canister approximately 3/4" from the rounded edge, avoiding the exact center. Turn the canister over and repeat.

A7.9.2. TO SMASH: Place bagged canisters inside a canvas bag, or wrap loosely in a protective cloth, before smashing. Check to assure both flat sides are destroyed.

A7.10. Locally reproduce this instruction and provide a copy to each user issued key in canisters.