

1 JANUARY 1998



Communications and Information

**CONTROLLING AUTHORITIES FOR COMSEC
KEYING MATERIAL (KEYMAT)**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: HQ AFCA/GCIS (MSgt Crowe)
Supersedes AFI 33-215, 1 August 1996

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 26
Distribution: F

This instruction outlines responsibilities of personnel who control (controlling authorities) communications security (COMSEC) keying material (keymat). It describes the roles of Director, National Security Agency (DIRNSA), Headquarters Cryptologic Systems Group (HQ CPSG), Headquarters Air Force Communications Agency (HQ AFCA), major commands (MAJCOM), and COMSEC managers, and controlling authorities in controlling COMSEC keymat. It also implements National Security Telecommunications and Information System Security Instruction (NSTISSI) No. 4006 (FOUO), *Controlling Authorities for COMSEC Material*. It takes precedence over all other Air Force publications affecting COMSEC controlling authorities. Send recommended changes to HQ AFCA/GCI, 203 West Losey Street, Rm 2040, Scott AFB IL 62225-5234. Refer conflicts between this and other instructions to HQ AFCA/XPPX, on AF Form 847, **Recommendation for Change of Publication**. MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) send one copy of their supplements to HQ AFCA/GCI, and HQ AFCA/XPPX.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision deletes instructions on operating and managing Communications-Electronic Operation Instructions, Joint Communications-Electronic Operation Instructions, and Signal Operation Instructions. It deletes roles of the National Security Agency (NSA) as a separate attachment and adds it as paragraph 4. Attachment 2 is updated and includes procedures for keymat usage, two person integrity, sensitive compartmented information, changing the classification of keymat, how to identify test or maintenance keymat for established systems, precautionary supersession, implementing when directed keymat, procedures for COMSEC incidents, and compromise recovery. It changes the references of Hotel Juliet (HJ) time to key change time. Attachments are added that provide examples for requests to establish a new keymat, increasing and decreasing copies of a keymat, deactivation of a cryptonet, precautionary supersession of a keymat, implementing a when directed keymat and revalidation of a keymat.

Report Documentation Page

Report Date 01 Jan 1998	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Air Force Instruction 33-215 Communication and Information Controlling Authorities for Comsec Keying Material (KEYMAT)		Contract Number
		Grant Number
		Program Element Number
Author(s)		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the AirForce Pentagon Washington D C 20330-1250		Performing Organization Report Number
Sponsoring/Monitoring Agency Name(s) and Address(es)		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified		Classification of this page unclassified
Classification of Abstract unclassified		Limitation of Abstract UU
Number of Pages 26		

1. Introduction . This instruction establishes responsibilities for controlling authorities of keymat and provides guidelines for compromise recovery. It describes functions and lists options for reacting to emergency or crisis situations and tells how to evaluate COMSEC incidents. The term MAJCOM when used in this publication, includes FOAs and DRUs. A glossary of references, abbreviations, acronyms, and terms is at Attachment 1.

2. Applicability and Scope. This instruction applies to all Air Force personnel assigned or acting as, controlling authorities to oversee and manage operational use and control of COMSEC keymat. Manage Joint Staff Intertheater COMSEC Package (JSICP) material according to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.03(C), *CJCS-Controlled Intertheater COMSEC Support (U)*. Manage positive control material according to CJCSI 3260.01(S), *Joint Policy Governing Positive Control Material and Devices (U)*.

3. Controlling Authority Appointment. When establishing a new cryptonet, identify a controlling authority to manage the operational use of the keymat assigned to the cryptonet. Whenever possible, ensure the controlling authority is organizationally senior to cryptonet members. The controlling authority must have the expertise to perform essential management functions and must have the authority to ensure its instructions are carried out. All cryptonet members, including those from other services or agencies, must comply with directions given by the controlling authority.

3.1. Since a cryptonet supports an operational requirement, assign controlling authority responsibilities to the operational organization directly supported by, or most closely associated with, the cryptonet.

3.2. For locally generated electronic key, the organization directing key generation performs the controlling authority functions, unless those functions are specifically assigned to another organization.

3.2.1. Only assign COMSEC accounts as controlling authority for keymat electronically generated by the account for its own use. **NOTE:** Do not assign MAJCOM Information Protection offices as controlling authorities.

3.3. Headquarters, United States Air Force (HQ USAF) and MAJCOMs may direct changes in controlling authority appointments under their control. Whoever directs these changes notifies all cryptonet members, appropriate distribution authorities, HQ CPSG/ZCK and DIRNSA/Y132, of all controlling authority appointments and changes.

4. Director, National Security Agency (NSA) Responsibilities.

4.1. Perform controlling authority functions for specified keymat generated by NSA facilities.

4.2. Take or recommend appropriate action when COMSEC material is subjected to compromise, and notify appropriate authorities of such actions.

4.3. When requested, assist controlling authorities in their annual cryptonet review.

4.4. Advise controlling authorities of the logistic impact of compromise, supersession, or other controlling authority decisions, in coordination with the appropriate distribution authorities.

5. Headquarters, Cryptologic Systems Group (HQ CSG) Responsibilities.

5.1. Act as the central office of record for all Air Force COMSEC accounts.

5.2. Provide overall management support for COMSEC material held by Air Force, Defense Logistics Agency, and Federal Aviation Administration COMSEC accounts.

5.3. Advise controlling authorities of the logistic impact of compromise, supersession, or other controlling authority decisions, in coordination with the appropriate distribution authorities.

5.4. Assist controlling authorities in their annual cryptonet review, when requested.

5.5. Send urgent messages to COMSEC accounts, MAJCOMs, and other concerned commands or agencies. Transmit messages by using MAJCOM address indicator groups or by sending directly to COMSEC accounts.

5.5.1. Transmit notices of compromised or replaced COMSEC material, including disposition instructions, when applicable.

5.5.2. Provide instructions for making encrypted-traffic review because of declared compromises of COMSEC material.

5.5.3. Transmit notices of non-routine supersession and changes of effective date.

5.5.4. Issue COMSEC publication amendments that require immediate implementation.

5.5.5. Update all status publications.

5.5.6. Perform other procedural and operational changes when immediate action is necessary.

6. Headquarters, Air Force Communications Agency (HQ AFCA) Responsibilities.

6.1. Act as HQ USAF COMSEC Incident Management Office.

6.1.1. Evaluate all reported physical COMSEC incidents involving multiple Air Force controlling authorities.

6.1.2. Maintain a record of COMSEC incidents reported by units within the Air Force.

6.1.3. Ensure all actions required of those units are completed.

7. Major Command Responsibilities.

7.1. The MAJCOM Information Protection office is the overseeing office. They will:

7.1.1. Determine controlling authority for cryptonets if one is not identified using the criteria in paragraph 3.

7.1.2. Direct changes to controlling authorities, if necessary.

7.1.3. Evaluate COMSEC incidents according to Air Force Instruction (AFI) 33-212, *Reporting COMSEC Incidents*.

8. Communication Security Manager Responsibilities.

8.1. Assist controlling authorities with COMSEC incidents, establishing new keymat (see Attachment 4), and understanding COMSEC Material Control System (CMCS) channels.

8.2. Provide extracts to status publications (AFKAG 11, *Index and Status of KG-84A/C K1V-7 Operations, On-The-Air Test, and Maintenance Test Keying Systems(U)*), through AFKAG 16, *Index and*

Status of Operational, Test and Maintenance Data Keys (U)) to the controlling authorities for the keymat they control. (See Attachment 5 to increase keymat and Attachment 6 to decrease keymat.)

8.3. Assist with local reproduction of manual crypto systems.

8.4. Know who has controlling authority responsibilities on their base.

8.5. Advise controlling authorities regarding proper COMSEC logistic procedures.

9. Controlling Authority Responsibilities and Cryptonet Management. Controlling authority responsibilities and cryptonet management procedures are in Attachment 2. Controlling authorities are allowed direct communications with cryptonet members. Controlling authorities must keep accurate records of all holders in order to assess the impact of, and recover from, a compromise. This includes:

9.1. Establishing a new cryptonet.

9.2. Cryptonet member identities and the amount of keymat they hold.

9.3. Resupply requirements for the cryptonet.

9.4. Cryptoperiod extensions allowed (see Attachment 3).

9.5. Cryptonet activation and key implementation date.

9.6. Operational requirements for the cryptonet.

9.7. Key change time.

9.8. Spare group assignments for operations codes.

9.9. Any extracts or local copying of keymat allowed.

9.10. Procedures for defective keymat.

9.11. Precautionary supersession of keymat (see Attachment 8).

9.12. Compromise recovery and COMSEC incident evaluation.

9.13. Test or maintenance of keymat.

9.14. Two Person Integrity (TPI) and Sensitive Compartmented Information (SCI) handling of keymat.

9.15. Changing the classification of the keymat.

9.16. Distribution of the keymat.

9.17. Tactical and high risk situations.

9.18. Procedures on when directed (WD) and contingency keymat (see Attachment 9).

9.19. Revalidation (see Attachment 10).

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

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

AFPD 33-2, *Information Protection*

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

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting COMSEC Incidents*

AFI 33-216, *Management of Manual Cryptosystems*

AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will convert to AFI 33-324)

AFKAG 1, *Communications Security (COMSEC) Operations*

AFKAG 2, *Air Force COMSEC Accounting Manual*

AFKAG 11(S), *Index and Status of KG-84A/C K1V-7 Operations, On-The-Air Test, and Maintenance Test Keying Systems* (U)

AFKAG 12(S), *Index and Status of Data Encryption Standard (DES) Systems and Fascinator Land Mobile Radio (LMR) Systems* (U)

AFKAG 13(C), *Index and Status of COMSEC General, Operating and Maintenance Manuals* (U)

AFKAG 14(S), *Index and Status of COMSEC Operational, Exercise, and Training Material* (U)

AFKAG 15(S), *Index and Status of Space Related COMSEC Systems* (U)

AFKAG 16(S), *Index and Status of Operational, Test and Maintenance Data Keys* (U)

CJCSI 3260.01(S), *Joint Policy Governing Positive Control Material and Devices* (U)

CJCSI 6510.03(C), *CJCS-Controlled Intertheater COMSEC Support* (U)

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

NSTISSI No. 4005 (FOUO), *Safeguarding COMSEC Facilities and Material*

NSTISSI No. 4006 (FOUO), *Controlling Authorities for COMSEC Material*

NOTE:

Users may obtain CJCSI publications by writing to HQ USAF/XODP, 1480 Air Force Pentagon, Washington DC 20330-1480, or calling DSN 225-3820.

Abbreviations and Acronyms

AFI—Air Force Instruction

CFD—Common Fill Device

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CMCS—COMSEC Material Control System
COMSEC—Communications Security
CRO—COMSEC Responsible Officer
DIRNSA—Director, National Security Agency
DRU—Direct Reporting Unit
DSN—Defense Switched Network
DTD—Data Transfer Device
FOA—Field Operating Agency
HQ AFCA—Headquarters Air Force Communications Agency
HQ AFCIC—Headquarters Air Force Communications and Information Center
HQ CPSG—Headquarters Cryptologic Systems Group
HQ USAF—Headquarters United States Air Force
JSICP—Joint Staff Intertheater COMSEC Package
keymat—Keying material
MAJCOM—Major Command
NSA—National Security Agency
NSTISSI—National Security Telecommunications and Information Systems Security Instruction
SCI—Sensitive Compartmented Information
STU-III—Secure Telephone Unit III
TPI—Two Person Integrity
USNDA—United States National Distribution Authority
WD—When Directed

Terms

All Holders—Consists of all cryptonet members, the supporting COMSEC accounts and MAJCOM of the supporting COMSEC account.

COMSEC Incident—Any occurrence that has the potential to jeopardize the security of COMSEC material or the secure electrical transmission of national security information.

COMSEC Incident Management Office—The office within the Air Force (HQ AFCA/GCIS) that maintains a record of COMSEC incidents caused by units within the Air Force and ensures units complete all required actions.

Cryptonet—Stations that hold a specific key for operational use.

Cryptonet Member—An individual station, among a group of stations, holding a specific key for use. Controlling authorities are actual cryptonet members. Cryptonet members are also referred to as users.

Cryptosystem—Associated COMSEC items interacting to provide a single means of encryption or decryption. (A cryptosystem can be a keyed COMSEC equipment, a code, or an authenticator.)

Distribution Authorities—Distribution points that ship keymat. US National Distribution Authority (USNDA) ships most keymat, and DIRNSA maintains it. Within the Air Force, HQ CPSG ships general publications and equipment.

Hard Copy Keymat—Keying material in physical form.

Keying Material (Keymat)—Key, code, and authentication information in physical or magnetic form.

Joint Staff Positive Control Material and Devices—A generic term referring to Sealed Authenticator Systems, Permissive and Devices Action Link, Coded Switch System, Positive Enable System, and Nuclear Certified Computer Data material or devices.

Attachment 2

CRYPTONET MANAGEMENT PROCEDURES

A2.1. Establishing New Keymat. Controlling authorities establish cryptonets with HQ CPSG/ZCK and advise DIRNSA/Y132 and all holders of the quantity of keymat needed (see Attachment 4). For manual cryptosystems (one-time pads, operations codes, authentication systems, etc.), controlling authorities must first identify specific operational requirements to HQ AFCA/GCI according to AFI 33-216, *Management of Manual Cryptosystems*.

A2.2. Activating a Cryptonet. If the initial implementation and supersession dates are not provided by the controlling authority, HQ CPSG/ZCK will designate this information. **NOTE:** NSA establishes supersession rates based on security, operational need, production and resupply constraints. Except in emergencies, controlling authorities cannot change supersession rates. A controlling authority may extend the effective dates of an edition to make use of spare settings when resupplies are uncertain.

A2.3. Cryptonet Configuration. Controlling authorities keep a record of all cryptonet members and prescribe the quantity of keymat for each member. This requires:

A2.3.1. Keeping detailed records of all cryptonet members to include identification of each cryptonet member, supporting COMSEC account, and numbers of copies held by each cryptonet member.

A2.3.2. Knowing problems cryptonet members may experience with the keymat.

A2.3.3. Knowing the distribution authorities that support the holders of the material and the fastest ways of issuing supersession and other emergency information to all holders of the keymat.

A2.3.4. Seeking assistance from the COMSEC manager on distribution and COMSEC channels.

A2.3.5. Telling HQ CPSG/ZCK, DIRNSA/Y132, and all holders of changes as controlling authority.

A2.3.5.1. Status publications contain controlling authority information. Status publications are maintained at COMSEC accounts only. Controlling authorities must ensure their information is up-to-date and accurate. Information includes: Points of contact, defense switched network (DSN) and commercial phone numbers, unit and office symbol, mailing address, message address, e-mail address, fax phone numbers (classified and unclassified), etc. (See Attachment 4.)

A2.3.6. Notifying all cryptonet members, HQ CPSG/ZCK, and DIRNSA/Y132 of any changes in cryptonet configuration or keymat status. If manual cryptosystems are concerned, controlling authorities must also notify DIRNSA/V31.

A2.4. Operational Requirements. Controlling authorities must know the operational requirements supported by the cryptonet and the proper use of the key. Controlling authorities must stay familiar with the operation and capabilities of the associated equipment.

A2.5. Keymat Usage. Controlling authorities will provide destruction, holding, etc. instructions to all cryptonet members on usage of the keymat. Keep a letter or message on file when keymat usage is different than prescribed within the operation instructions for that specific cryptosystem.

A2.6. Two Person Integrity. Controlling authorities must ensure that TOP SECRET keymat is handled under TPI procedures as outlined in AFI 33-211, *Communications Security (COMSEC) User Requirements*.

A2.7. Sensitive Compartmented Information. Controlling authorities will designate keying material used for encryption of SCI. Notify all cryptonet members of the correct handling of this material.

A2.8. Changes in Classification. Controlling authorities will approve changes in classification of the key if the classification is downgraded. First, coordinate any upgrades to the classification with HQ CPSG/ZCK. Before upgrading keying material to TOP SECRET, controlling authorities must ensure that material is protected under TPI procedures and that all personnel and facilities are cleared for the TOP SECRET level.

A2.9. Key Change Time. Controlling authorities will specify key change time for the cryptonet when the time is not prescribed in the keymat. The time selected for key change must have the least operational impact on the cryptonet. Keep the time selected for key change consistent throughout the cryptonet. If key change time is not specified, it is 0001Z. Additionally, controlling authorities may change key change time by notifying the cryptonet members.

A2.10. Spare Group Assignment. Controlling authorities make spare group assignments of operations codes, as necessary. Notify all cryptonet members of all changes and ensure changes are included in future production copies.

A2.11. Key Distribution. Controlling authorities prescribe electronic generation and distribution of keys (except key encryption keys.) They also prescribe physical transfer of keys in a common fill device, or local reproduction of keys, when established channels cannot supply the material in time to meet urgent operational requirements. Controlling authorities make sure reproduced material is kept to the minimum essential amount and is properly classified, controlled, and destroyed as applicable. Controlling authorities obtain register numbers from HQ CPSG/ZCK for copies of Accounting Legend Code-1 material reproduced by Air Force COMSEC accounts. Controlling authorities who routinely allow reproduction of the same material must increase the copy count of that material.

A2.12. Test or Maintenance Keymat. AFKAG 13(C), *Index and Status of COMSEC General, Operating and Maintenance Manuals(U)* lists the test, maintenance, and training keys for established cryptosystems. Detailed information is also provided for these keymats in the following publications, maintained by the COMSEC account: AFKAG 11 (S), AFKAG 12 (S), *Index and Status of Data Encryption Standard (DES) Systems and Fascinator Land Mobile Radio (LMR) Systems(U)*, AFKAG 14 (S), *Status and Index of COMSEC Operational, Exercise and Training Material (U)*, AFKAG 15 (S), *Index and Status of Space Related COMSEC Systems (U)*, and AFKAG 16 (S).

A2.13. Resupply. Controlling authorities coordinate with distribution authorities to make sure of timely resupply of keymat. Controlling authorities must:

A2.13.1. Promptly check the status of follow-on material when notified by a COMSEC account that they have only a two month supply of keymat or two segments of material for annually superseded material.

A2.13.2. Direct cryptonet members to implement the longest authorized cryptoperiod extension for each remaining key setting if COMSEC accounts are not assured of resupply before their remaining key is superseded (see paragraph A2.14).

A2.13.3. If the extension is not enough or the resupply date is not determined, controlling authorities must report, by IMMEDIATE precedence message, to HQ CPSG/ZCK, INFO: DIRNSA/V51A/Y132. This allows responsible agencies to make contingency arrangements. The message must include:

A2.13.3.1. The keymat short title.

A2.13.3.2. Number of cryptonet members.

A2.13.3.3. Description of the type of operations (for example, full-time, or part-time, fixed or mobile communications center).

A2.13.3.4. Explanation of the necessity for the cryptoperiod extension.

NOTE: When time is critical, controlling authorities may verbally request emergency cryptoperiod extensions from NSA/V511 DSN/STU-III 244-6831; commercial/STU-III (410) 859-6831. When authorized verbally, controlling authorities must take immediate action and not wait for message documentation. Cryptonet members abide by verbal instructions relayed by controlling authorities.

A2.14. Extensions. Controlling authorities for manual cryptosystems can extend the cryptoperiod by 72 hours. Controlling authorities for automanual and machine cryptosystems can extend the cryptoperiod by one week. That is, controlling authorities can add either 72 hours or one week, as applicable, to the regular cryptoperiod, unless the specific cryptosystem doctrine prohibits cryptoperiod extensions or authorizes a longer extension. Controlling authorities are not required to report these extensions to HQ CPSG or DIRNSA, unless there is a change in the effective dates. Cryptonet members can extend cryptoperiods up to two hours to complete a transmission or conversation in process at key change time. Controlling authority approval is not required and cryptonet members are not required to report these extensions (see Attachment 3.)

A2.15. Precautionary Supersession. When the controlling authority determines that a compromise of keymat has occurred, (for example, material was stolen, passed over non-secure means, etc.), notify HQ CPSG/ZCK, DIRNSA/Y132, and all holders. See Attachment 8 for example of a precautionary supersession message. All holders will advance to the next segment or edition, as determined by the controlling authority. Send an immediate precedence message to advise of this change. COMSEC managers will immediately pass messages and additional keymat, if needed, to cryptonet members.

A2.15.1. Direct the emergency supersession of keymat under their control according to Attachment 2 and Attachment 8, and immediately notify HQ CPSG/ZCK and DIRNSA/Y132.

A2.15.2. Coordinate with HQ CPSG/ZCK prior to superseding key to make sure adequate material is available to all holders to support future needs.

A2.16. Extracts. Controlling authorities approve the number of extracts of keymat issued to a cryptonet member at any one time, except where specified in the material. Issue protectively packaged keymat as entire editions, except where operational necessity prevents such issue. Removing keymat from its protective packaging defeats the purpose of protective packaging and exposes the key to unauthorized copying.

A2.17. Tactical and High Risk Situations.

A2.17.1. Tactical Situations. Issue keymat in ample quantities to support mission requirements. Issue it in either hard copy or electronic form depending on the risk, as determined by the local commander. Use any multiple key storage capacity of the equipment. If equipment does not have multiple fill capacity, or has insufficient capacity, issue common fill device (CFD) (KYK-13 or KYX-15) or data transfer device (DTD) (AN/CYZ-10 or AN/CYZ-10A). If hard copy keymat is issued, issue extracts when only a few settings are required, otherwise issue the entire edition. Base your decision of whether to issue extracts or entire editions on a risk assessment and careful consideration of the logistic problems associated with emergency resupply due to compromise.

A2.17.2. High Risk Situations. Issue keys in electronic form.

A2.18. Reproduction of COMSEC Material for Manual and Machine Cryptosystems.

A2.18.1. Manual Cryptosystems. COMSEC managers may locally reproduce manual cryptosystems (that is, codes and authenticators) for validated users as necessary to meet operational needs. You must have controlling authority approval to reproduce sealed manual cryptosystems. Reproduce and control manual cryptosystems according to instructions in AFKAG-14(S). **NOTE:** Reproduction occurs when complete editions are reproduced. When the complete edition is not reproduced, it is considered an extract (see A2.16).

A2.18.2. Machine Cryptosystems. Do not reproduce keying material for machine cryptosystems without the consent of the controlling authority. If you cannot obtain controlling authority approval in time to meet operational requirements, or if a controlling authority is not designated, the local commander may authorize reproduction. Notify the controlling authority at the earliest opportunity. COMSEC managers will obtain register numbers of account legend code 1 material from HQ CPSG/ZCK, and account for the reproduced material according to AFKAG-2, *Air Force COMSEC Accounting Manual*. **NOTE:** For JSICP material, contact the JSICP manager for accounting control numbers.

A2.19. Defective Keymat. Controlling authorities and cryptonet members will report defective keymat immediately to their supporting COMSEC manager. Include in the report a full description as to what is wrong with the material, if known, or the reason for submitting the report. The COMSEC manager submits the report according to AFI 33-212.

A2.19.1. Provide the material to the COMSEC manager, who will keep the defective material and all associated packaging materials until disposition instructions are received. The COMSEC manager will return the recalled keymat, upon request from the proper authority, by approved shipping methods as prescribed in AFKAG-2. Transfer reports must state the authority. Refer to the recall message and include any other remarks requested in the recall message.

A2.19.2. Controlling authorities must determine if they need to supersede (e.g., found several defective key canisters) or if users can continue to operate using the current material.

A2.20. When Directed (WD) Keymat. Until keymat is implemented, it is placed in a WD status. Once the circuit is activated, the keymat is implemented and all holders, HQ CPSG/ZCK and DIRNSA/Y132 are notified. When known circuit outages will cause an extended amount of outage time (e.g., two or three months), the controlling authority places the keymat in WD status. Irregularly used keymat (e.g.,

EAM codes, telemetry keymat, etc.), will generally have an effective edition in use for an undetermined period of time while the follow-on editions remain in WD status until the controlling authority implements one or more editions. This way you can save unused keymat from unnecessary supersession or destruction. Substantial savings in production, distribution, accounting, and destruction are possible when unused keymat is placed in a WD status.

A2.21. Contingency Keymat. Hold contingency keymat in WD status until called out and implemented for a crisis, contingency or exercise. Activate keymat when needed for the specific requirement, destroy it after it is superseded, and place it back into a WD status until it is called out and implemented again.

A2.22. Revalidation. Controlling authorities carry out annual revalidation of keymat, used with machine cryptosystems, to confirm cryptonet structure, quantities and adequacy of the key to meet operational requirements, and continuing requirement for the key. Send revalidations to the cryptonet members and COMSEC accounts with INFO to the COMSEC accounts supporting MAJCOM (see Attachment 10). Deactivate the cryptonet if no longer needed (see Attachment 7). During the revalidation, identify cryptosystems of low peacetime use that are candidates for placement into WD status. Revalidate keymat for manual cryptosystems according to AFI 33-216. Send a summary of each revalidation to HQ CPSG/ZCK.

A2.23. COMSEC Incidents. Controlling authorities must ensure cryptonet members are trained to recognize COMSEC incidents and immediately report them to the COMSEC manager. When keying material is used by other than Air Force cryptonet members, those cryptonet members must know to report COMSEC incidents according to service instructions. They must also address reports to HQ AFCA SCOTT AFB IL//GCIS//. **NOTE:** COMSEC Incident reporting is exempt from licensing according to AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will convert to AFI 33-324).

A2.23.1. Controlling authorities will review and evaluate COMSEC incidents to all addressees of the initial COMSEC incident report.

A2.23.1.1. Evaluate and respond to initial reports of the following incidents within 24 hours:

A2.23.1.1.1. Currently effective keymat or keymat that is effective within 15 days.

A2.23.1.1.2. Defection, espionage, hostile cognizant agent, clandestine exploitation, tampering, penetration or sabotage, or unauthorized copying, reproduction, or photography.

A2.23.1.2. Evaluate and respond to initial reports of the following incidents within 48 hours:

A2.23.1.2.1. Future keymat that becomes effective beyond the next 15 days.

A2.23.1.2.2. Superseded, reserve, or contingency keymat.

A2.23.1.2.3. Evaluate and respond to initial reports of COMSEC incidents not covered above within 5 duty days.

A2.23.2. Use the COMSEC Incident Evaluation Guide in AFI 33-212 to evaluate COMSEC incidents.

A2.24. Compromise Recovery. Compromise recovery and incident evaluation are two separate, distinct actions required of a controlling authority. Where substantial evidence of compromised COMSEC mate-

rial exists, controlling authorities must take immediate action. Controlling authorities will not wait for receipt of incident reporting and evaluating requirements, but will initiate recovery action when they have enough information to make an informed decision. Ideally, controlling authorities will announce precautionary supersession (see Attachment 8).

A2.24.1. The feasibility of superseding hard copy keying material is contingent on several factors: the number of editions held at the user level, the capability of NSA to produce keying material, and the distribution authority's capability to supply replacement editions. Any decision to supersede must take into consideration the time required to notify all cryptonet members and implement the new material. Report emergency supersession of hard copy key immediately to appropriate distribution authorities, HQ CPSG/ZCK and DIRNSA/Y132 so that they can take resupply action, produce replacement material, and correct status documents.

A2.24.2. Superseding locally generated electronic key can present a unique problem for mobile or tactical users. Some of the communications paths used to deliver the key may no longer exist due to the redeployment of some of the relaying units. The controlling authority must consider the time needed to create or re-establish communications paths before directing supersession.

A2.24.3. The following options are available to controlling authorities when supersession is warranted, but not all cryptonet members hold replacement key. In order of preference:

A2.24.3.1. Electronically generate key and transmit to cryptonet members via an uncompromised cryptosystem approved for over-the-air key transfer.

A2.24.3.2. Transmit printed key settings by a cryptosystem that provides end-to-end encryption equal to the classification of the transmitted key (e.g., the Automatic Digital Network system, secure facsimile, or secure telephone). Encrypt printed key settings by automanual or one-time pad system and transmit over a system secured at a lower level than the encrypted key.

A2.24.3.3. Reproduce printed key settings and physically transfer to cryptonet members. Do not reproduce punched tape without the authorization of DIRNSA/V51. Converting hard copy keying material to electronic form for equipment fill is not considered reproduction.

A2.24.3.4. Transfer physical key to cryptonet members in a CFD or DTD. When keyed, users must protect the CFD at the same level as the highest classification level of the key it contains. Refer to AFSSI 3021, (FOUO) *Interim Operational Security Doctrine for the AN/CYZ-10/A Data Transfer Device (DTD)*, for handling and classification of the DTD.

A2.24.4. When precautionary supersession is not feasible, several options are available to the controlling authority. In order of preference, the controlling authority may:

A2.24.4.1. Extend the cryptoperiod of uncompromised keying material in accordance with A2.14 and Attachment 3.

A2.24.4.2. Exclude from cryptonet operations those members who do not hold or are not furnished replacement material.

A2.24.4.3. Suspend cryptonet operations until key is resupplied.

A2.24.4.4. Continue to use the compromise key. This action is a last resort when normal supersession of the compromised material will take place before emergency supersession can occur or where keying material changes have a serious detrimental effect on operations, or where no replacement material is available. The controlling authority must alert cryptonet members (by

other secure means if available) that a possible compromise has taken place and direct that members minimize transmissions using the compromised key. **NOTE:** Use this option only when continued cryptonet operation is absolutely essential to the mission.

A2.24.5. Controlling authorities will direct traffic reviews of record traffic encrypted in compromised keying material when warranted.

A2.24.5.1. When a traffic review is directed, all cryptonet members must evaluate all traffic for the time period involved. Determine what level of traffic and the amount of information that was compromised. The cryptonet members gather the information and send a message to the controlling authority with INFO to the supporting COMSEC account, HQ CPSG/ZCK, and supporting COMSEC accounts MAJCOM.

Attachment 3

GUIDELINES FOR EXTENDING CRYPTOPERIODS

A3.1. Extensions. When you must extend cryptoperiods for reasons other than logistics needs (for example, under pre-strike, battlefield, or field training conditions), controlling authorities are encouraged to conduct a risk assessment prior to implementing the extension. Controlling authorities should consider the following factors before making a decision as to the length of time they will extend the cryptoperiod.

A3.1.1. Size of the Cryptonet. The key used on a large cryptonet is usually more vulnerable to compromise than the key used on a small cryptonet because it is available at more locations and more people have access to it. Also, large nets generally carry higher volumes of traffic than small nets. The compromise of a key used to secure a large net could make more intelligence available to an adversary. For this reason, controlling authorities must keep their cryptonets as small as operationally feasible.

A3.1.2. Location and Operating Environment of Cryptonet Members. Cryptonet members located in the United States, its territories, and its protectorates are normally at less risk than those in other locations. Cryptonet members located in high risk environments (that is, areas outside the United States where there is a small or no United States or allied military presence or where the political climate is unstable) have an increased risk of physical compromise. Mobile and tactical users have a greater opportunity for loss (particularly undetected loss) of material than fixed cryptonet members. In addition, loss on the battlefield could pose an immediate threat not only to United States communications but also to United States lives.

A3.1.3. Sensitivity and Perishability of Traffic. The controlling authority should consider the classification of the protected information, and whether the information is of long-or-short term intelligence value. Compromising a key used to secure upper level strategic communications would have a more devastating effect on United States security than compromising a key used to secure highly perishable or lower level tactical communications.

A3.1.4. Emergency Supersession Plan. The controlling authority must have a plan for replacing compromised key. They must know approximately how quickly they can replace the key if the plan is realistic in a worst case scenario. The controlling authority must establish procedures for rekeying the net, because it is extremely difficult to accomplish an unscheduled rekey in a large net without creating additional problems and confusion. The controlling authority must know the CMCS channels that support the cryptonet as well as the electronic key transfer or distribution capabilities of the associated equipment.

A3.1.5. Operation Impact of an Extended Cryptoperiod. The controlling authority must make an assessment as to whether extending the cryptoperiod is for operational necessity. Do not extend cryptoperiods for operator's convenience. If we do not follow standard procedures during wartime, the value of our peacetime training is questionable.

A3.2. If cryptoperiod extensions are necessary to maintain critical communications during battle (actual or field training), the following guidelines apply:

A3.2.1. Begin all cryptoperiods with a new key setting.

A3.2.2. Extend cryptoperiods by net and not by short title, whenever possible.

A3.2.3. Rekey all affected nets when there is a break in activity.

Attachment 4

SAMPLE REQUEST TO ESTABLISH NEW KEYMAT

DTG

FM (Controlling Authority)

TO HQ CPSG SAN ANTONIO TX//ZCK//

INFO DIRNSA FT GEORGE G MEADE MD//Y132//

(Supporting COMSEC Account of Cryptonet Member)*

(MAJCOM of COMSEC Account)*

(Cryptonet Member)*

BT

UNCLAS

MSGID/GENADMIN/(Controlling Authority)/-/JUN//

SUBJ/REQUEST TO ESTABLISH A NEW KEYING SYSTEM//

REF/A/(Letter, Message or OPlan, etc.)

POC/(Name)/(Position or Title)/(Unit/FAS)/LOC: (Base)/DSN: (Phone Number)/

RMKS/1. THIS REQUEST IS SUBMITTED ACCORDING TO AFI 33-215:

A. KEYING MATERIAL REQUIRED:

(1) SHORT TITLE: UNKNOWN

(2) TYPE OF EQUIPMENT: (List Specific Equipment)

B. USERS/COMSEC ACCOUNT/NUMBER OF COPIES:

(1) (Cryptonet Member)/(Supporting COMSEC Account)/(Number of Copies per User)

(2) (Cryptonet Member)/(Supporting COMSEC Account)/(Number of Copies per User)

(3) (Cryptonet Member)/(Supporting COMSEC Account)/(Number of Copies per User)

C. CONTROLLING AUTHORITY INFORMATION:

(1) UNIT/OFFICE SYMBOL: (Controlling Authority)

(2) MESSAGE ADDRESS: (Message Address from TO Line)

(3) MAILING ADDRESS: (Unit/FAS of Controlling Authority)

(Street Address and Suite or Room Number)

(Base) (State) (Zip Code + 4)

(4) POC: (Full Name and Rank)

(5) E-MAIL ADDRESS: (Give Full Internet E-mail Address)

(5) PHONE NUMBERS: DSN: (Phone Number)

COMMERCIAL: (Area Code + Phone Number)

(6) FAX NUMBERS: SECURE: (Phone Number)

UNCLAS: (Phone Number)

D. HIGHEST CLASSIFICATION LEVEL OF TRAFFIC YOU WANT TO TRANSMIT: {TOP SECRET, SECRET, CONFIDENTIAL, UNCLAS}

E. SPECIAL HANDLING: {US RELEASE ONLY, RELEASABLE TO US/UK, SCI, etc.}

F. DESIRED SUPERSESSION RATE PER EDITION: {YEARLY, QUARTERLY, BI-MONTHLY, MONTHLY}

G. DESIRED CRYPTOPERIOD PER SEGMENT: {QUARTERLY, WEEKLY, DAILY}

H. REQUESTED IN-PLACE DATE: (DD MMM YY)

I. INITIAL IMPLEMENTATION DATE: (DD MMM YY)

2. JUSTIFICATION: (Give complete justification as to why this keymat is needed)

3. AUTHORITY: (List an OPlan, message, etc.)

4. PURPOSE: (CPSG will list this information in the status publications for the purpose of this keymat)

5. GENERAL OR AMPLIFIED COMMENTS: (Give any special instructions in this area. Coordinate requests with all supporting COMSEC accounts and add a statement confirming coordination. Also indicate if it is anticipated that the number of cryptonet members will increase and additional copies of the system will be required, so that a system can then be assigned that will allow for expansion of the keymat without causing a delay.)

****Repeat this information for each member***

() - Give the information requested

{ } - Examples of information to place in these areas

Attachment 5

SAMPLE REQUEST FOR AN INCREASE IN KEYMAT

DTG

FM (Controlling Authority)

TO HQ CPSG SAN ANTONIO TX//ZCK// (If an Air Force COMSEC Account)

DIRUSACCSLA FT HUACHUCA AZ//SELCL-KPD-KEY// (If an Army COMSEC Account)**

DCMS WASHINGTON DC (If a Navy COMSEC Account)**

DIRNSA FT GEORGE G MEADE MD//Y132// (If an NSA COMSEC Account)**

INFO DIRNSA FT GEORGE G MEADE MD//Y132// (If not an action addressee)

(Supporting COMSEC Account of Cryptonet Member)*

(MAJCOM of COMSEC Account)*

(Cryptonet Member)*

BT

UNCLAS

MSGID/GENADMIN/(Controlling Authority)/-/JUN//

SUBJ/REQUEST TO INCREASE KEYMAT//

REF/A/(Message from COMSEC Account requesting increase)//

POC/(Name)/(Position or Title)/(Unit/FAS)/LOC: (Base)/DSN: (Phone Number)/

RMKS/1. THIS REQUEST IS SUBMITTED ACCORDING TO AFI 33-215:

A. COMSEC ACCOUNT:

B. KEYING MATERIAL:

Table A5.1. Remove This.

SHORTON HANDINCREASENEW

TITLEPER EDITIONLEVEL

USKAT-1234325

C. REQUESTED IN PLACE DATE: (DD MMM YY)

D. REQUEST INCREASE BEGIN WITH EDITION: (Give edition COMSEC account must have)

E. GENERAL AMPLIFIED COMMENTS: (Give any additional information if needed)

2. REQUEST HQ CPSG/ZCK UPDATE THIS ACCOUNTS USNDA DISTRIBUTION PROFILE FOR USKAT-1234, AS APPLICABLE.

3. UPON RECEIPT OF THE USNDA DISTRIBUTION PROFILE CHANGE(S), REQUEST NSA SHIP AN INCREASE LEVEL OF USKAT-1234 EDITIONS ALREADY TRANSFERRED TO MEET

THE REQUESTED IN-PLACE DATE AND SHIP INCREASED LEVELS BEGINNING WITH THE NEXT EDITIONS SHIPPED.

*** Repeat this information for each member.**

******Choose the appropriate agency depending on the supporting COMSEC account.

Service/AgencyFirst Digit

Navy0 thru 3

Army5

Air Force6 and 7

NSA8

NOTE: These examples are used by the controlling authorities. COMSEC managers must send their request to the controlling authorities with complete justification and their authority. See AFKAG-2 for examples.

Attachment 6

SAMPLE REQUEST FOR A DECREASE IN KEYMAT

DTG

FM (Controlling Authority)

TO HQ CPSG SAN ANTONIO TX//ZCK// (If an Air Force COMSEC Account)

DIRUSACCSLA FT HUACHUCA AZ//SELCL-KPD-KEY// (If an Army COMSEC Account)**

DCMS WASHINGTON DC (If a Navy COMSEC Account)**

DIRNSA FT GEORGE G MEADE MD//Y132// (If an NSA COMSEC Account)**

(Supporting COMSEC Account of Cryptonet Member)*

INFO DIRNSA FT GEORGE G MEADE MD//Y132// (If not an action addressee)

(MAJCOM of COMSEC Account)*

(Cryptonet Member)*

BT

UNCLAS

MSGID/GENADMIN/(Controlling Authority)/-/JUN//

SUBJ/REQUEST FOR A DECREASE IN KEYMAT//

REF/A/(Message from COMSEC Account requesting increase)//

POC/(Name)/(Position or Title)/(Unit/FAS)/LOC: (Base)/DSN: (Phone Number)/

RMKS/1. THIS REQUEST IS SUBMITTED ACCORDING TO AFI 33-215:

A. COMSEC ACCOUNT:

B. KEYING MATERIAL:

SHORTON HANDDECREASENEW

TITLEPER EDITIONLEVEL

USKAT-1234321

2. REQUEST HQ CPSG/ZCK UPDATE THIS ACCOUNTS USNDA DISTRIBUTION PROFILE FOR USKAT-1234, AS APPLICABLE.

3. (Unit/CA 612345): (Before providing disposition instructions, controlling authorities must coordinate with the system item manager at the distribution authority to determine how to administer disposition instructions. Consider the system's size [point-to-point, small network, widely-held system with numerous changes in quantity, etc.], net members [Air Force only, joint system, etc.], purpose [supports a specific project, supports many operations in several theaters, general document, etc.], and management [unfilled emergency requests, spare copies maintained for immediate distribution, limited number of copies available for distribution without additional production, etc.], decide who will provide the disposition [controlling authority or the service item manager], and the disposition instructions either destruction, transfer to another COMSEC account having a requirement for the material, or return back to distribution

point.) AUTHORITY IS GRANTED TO DESTROY ALL EXCESS COPIES OF USKAT-1234 ON-HAND AND ENROUTE.

4. GENERAL AMPLIFIED COMMENTS: (Give any additional information if needed)

****Repeat this information for each member.***

******Choose the appropriate agency depending on the supporting COMSEC account.

Service/AgencyFirst Digit

Navy0 thru 3

Army5

Air Force6 and 7

NSA8

NOTE: These examples are used by the controlling authorities. COMSEC managers must send their request to the controlling authorities with complete justification and their authority. See AFKAG-2 for examples.

Attachment 7

SAMPLE DEACTIVATION OF A CRYPTONET

DTG

FM (Controlling Authority)

TO HQ CPSG SAN ANTONIO TX//ZCK// (If an Air Force COMSEC Account)

DIRUSACCSLA FT HUACHUCA AZ//SELCL-KPD-KEY// (If an Army COMSEC Account)**

DCMS WASHINGTON DC (If a Navy COMSEC Account)**

DIRNSA FT GEORGE G MEADE MD//Y132// (If an NSA COMSEC account)

(Supporting COMSEC Account of Cryptonet Member)*

(Cryptonet Member)*

INFO DIRNSA FT GEORGE G MEADE MD//Y132// (If not an action addressee)

(MAJCOM of COMSEC Account)*

BT

UNCLAS

MSGID/GENADMIN/(Controlling Authority)/-/JUN//

SUBJ/USKAT-345 CANCELLATION//

REF/A/(Any information referencing this action - letter or message)//

POC/(Name)/(Position or Title)/(Unit/FAS)/LOC: (Base)/DSN: (Phone Number)/

RMKS/1. AS CONTROLLING AUTHORITY REQUEST CANCELLATION OF USKAT-345 EFFECTIVE IMMEDIATELY. THIS SYSTEM IS NO LONGER NEEDED.

2. PLEASE UPDATE THE USNDA PROFILE TO REFLECT THIS CANCELLATION.

3. ALL HOLDERS ARE AUTHORIZED TO DESTROY ALL COPIES ON-HAND AND ENROUTE.

****Repeat this information for all holders.***

****Choose the appropriate agency depending on the supporting COMSEC account.**

Service/AgencyFirst Digit

Navy0 thru 3

Army5

Air Force6 and 7

NSA8

Attachment 8

SAMPLE PRECAUTIONARY SUPERSESSION OF KEYMAT IMMEDIATE MESSAGE

DTG

FM (Controlling Authority)

TO HQ CPSG SAN ANTONIO TX//ZCK//

DIRNSA FT GEORGE G MEADE MD//Y132//

(Supporting COMSEC Account of Cryptonet Member)*

(Cryptonet Member)*

INFO (MAJCOM of COMSEC Account)*

BT

C O N F I D E N T I A L

MSGID/GENADMIN/(Controlling Authority)/-/JUN//

SUBJ/PRECAUTIONARY SUPERSESSION OF USKAT-1234//

REF/A/(Message or telecon informing of compromise)//

POC/(Name)/(Position or Title)/(Unit/FAS)/LOC: (Base)/DSN: (Phone Number)/

RMKS/1. (C) USKAT-1234, EDITION BRAVO (B) IS SUPERSEDED AT 2359Z, 20 JUN 97.

USKAT-1234, EDITION CHARLIE (C), SEGMENT 1A WILL BECOME EFFECTIVE AT 0001Z, 21 JUN 97. USKAT-1234, EDITION DELTA (D) WILL BECOME EFFECTIVE 1 AUG 97, WITH NORMAL SUPERSESSION THEREAFTER.

CLASSIFIED BY: AFMAN 33-272

DECLAS: X-1

****Repeat these items for all holders.***

Attachment 9

SAMPLE IMPLEMENTING A WHEN DIRECTED (WD) KEYMAT

DTG

FM (Controlling Authority)

TO DIRNSA FT GEORGE G MEADE MD//Y132//

HQ CPSG SAN ANTONIO TX//ZCK//

(Supporting COMSEC Account of Cryptonet Member)*

(Cryptonet Member)*

INFO (MAJCOM of COMSEC Account)*

BT

C O N F I D E N T I A L

MSGID/GENADMIN/(Controlling Authority)/-/JUN//

SUBJ/IMPLEMENTATION OF USKAT-2345//

REF/A/(Message or any reference requesting you implement the keymat)//

POC/(Name)/(Position or Title)/(Unit/FAS)/LOC: (Base)/DSN: (Phone Number)/

RMKS/1. (C) USKAT-2345, EDITION ECHO (E) IS EFFECTIVE FROM 1 JUL 97 THRU 31 AUG 97. USKAT-2345, EDITION FOXTROT (F) IS PLACED IN A WD STATUS.

2. (U) PLEASE UPDATE USKAT-2345 PROFILE TO REFLECT THIS CHANGE.

CLASSIFIED BY: AFMAN 33-272

DECLAS: X-1

****Repeat these items for all holders.***

Attachment 10

SAMPLE REVALIDATION

DTG

FM (Controlling Authority)

TO (Cryptonet Member)*

(Supporting COMSEC Account of Cryptonet Member)*

INFO (MAJCOM of COMSEC Account)*

BT

UNCLAS

MSGID/GENADMIN/(Controlling Authority)/-/JUN//

SUBJ/REVALIDATION OF USKAT-2345//

REF/A/AFI 33-215//

POC/(Name)/(Position or Title)/(Unit/FAS)/LOC: (Base)/DSN: (Phone Number)/

EACH ACTION ADDRESSEE MUST PROVIDE THE FOLLOWING INFORMATION NLT (Give approximately 30-45 days).

1. SUPPORTING COMSEC ACCOUNT NUMBER
2. CRO UNIT/OFFICE SYMBOL
3. TOTAL NUMBER OF COPIES RECEIVED FROM THE COMSEC ACCOUNT
4. SUPPORTING NETWORK (If point to point - state purpose of the net)
5. JUSTIFICATION FOR THE CRYPTONET (Give OPlan, OPR of the OPlan and date)
6. FREQUENCY OF USAGE (Daily, Weekly, WD, etc.)
7. KEY CHANGE TIME
8. USAGE - (Ground to Ground, Ground to Air, or Air to Air)
9. TYPE OF OPERATION - (Full-time, Part-time, Fixed or Mobile)
10. TYPE OF EQUIPMENT - (KG-84, KY-57, etc.)
11. ANY FUTURE ISSUES THAT MAY EFFECT COPY COUNT TO THE CRYPTONET MEMBER: (Moving, closing, increasing or decreasing copies, etc.)
12. OTHER COMMENTS: (Any additional information not covered above)

****Repeat these items for all holders.***