NSTISSI No. 4006
2 December 1991

NSTISS
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

CONTROLLING AUTHORITIES

FOR

COMSEC MATERIAL

~~FOR OFFICIAL USE ONLY~~

NSTISS
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

NATIONAL MANAGER

2 December 1991

FOREWORD

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4006, "Controlling Authorities for COMSEC Material," establishes the responsibilities of controlling authorities for keying material and for Communications-Electronics Operation Instructions (CEOI), Joint Communications-Electronics Operation Instructions (JCEOI), and Signal Operation Instructions (SOI).

2. This instruction supersedes NTISSI No. 4006, "Controlling Authorities for COMSEC Keying Material," dated 2 May 1989. It differs from the previous version in that it allows controlling authorities to approve longer cryptoperiod extensions without the concurrence of the National Security Agency (NSA), it authorizes local reproduction of manual cryptosystems without controlling authority approval, and it allows controlling authorities to approve changes in the classification of the material they control. Also, the guidelines and time limits for evaluating COMSEC incidents have been incorporated into NSTISSI No. 4003.

3. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

Executive Secretariat
National Security Telecommunications and Information
Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755-6000

4. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

5. Comments and suggestions regarding this NSTISSI may be sent directly to NSA ([redacted]), telephone [redacted] or DSN [redacted].

(b)(3)-P.L. 86-36

W. O. STUDEMAN
Vice Admiral, U.S. Navy

CONTROLLING AUTHORITIES FOR COMSEC MATERIAL

SECTION I - PURPOSE

1. Controlling authorities have certain responsibilities and prerogatives relating to the material they control. This instruction establishes those responsibilities and provides guidelines for compromise recovery.

SECTION II - SCOPE

2. The requirements of this NSTISSI apply to all U.S. Government departments and agencies and their agents, which include, but are not limited to, contractors, consultants, and licensees. Its specific requirements apply to controlling authorities for keying material used to secure classified information or information as set forth in 10 U.S.C. Section 2315, Communications-Electronics Operation Instructions (CEOI), Joint Communications-Electronics Operation Instructions (JCEOI), and Signal Operation Instructions (SOI). The requirements apply to all the aforementioned material, irrespective of form or generation process, except as specified in paragraph 3.

3. The requirements of this NSTISSI do not apply to controlling authorities for Joint Staff positive control material and devices. Controlling authorities for Joint Staff positive control material and devices must follow the requirements of Joint Pub 1-04.

SECTION III - REFERENCES

4. This instruction refers to the following publications:

a. NACSI No. 4005, Safeguarding and Control of Communications Security Material, dated 12 October 1979.

b. NCSC-9, National COMSEC Glossary, dated 1 September 1982.

c. Joint Pub 1-04, Joint Policies and Procedures Governing Positive Control Material and Devices, dated 1 August 1990.

d. NSTISSI No. 3014, Management of Off-line Cryptosystems, dated 1 February 1991.

e. NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991.

SECTION IV - DEFINITIONS

5. The definitions contained in NCSC-9 apply to this instruction. The following definitions also apply to this NSTISSI.

a. COMSEC Incident. Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 U.S.C. Section 2315.

b. COMSEC Incident Monitoring Activity. The office within a department or agency that maintains a record of COMSEC incidents caused by elements of that department or agency, and ensures that all actions required of those elements are completed.

c. Cryptonet. Stations that hold a specific key for use.

d. 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.)

e. [redacted]

f. Keying Material. Key, code, or authentication information in physical or magnetic form.

SECTION V - CONTROLLING AUTHORITY APPOINTMENT

6. When a new cryptonet is established, a controlling authority will be identified to manage the operational use of keying material assigned to the cryptonet. The controlling authority should be 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 net members, including members from other departments or agencies, must adhere to the direction given to the cryptonet by the controlling authority.

7. Since a cryptonet supports an operational requirement, the operational organization directly supported by, or most closely associated with, the cryptonet will normally be assigned controlling authority responsibilities. COMSEC managers are normally inappropriate candidates for assignment as controlling authority, because typically they are not familiar with net membership and operational requirements. However, COMSEC managers will advise controlling authorities regarding proper COMSEC logistics procedures.

8. A controlling authority will also be identified for each CEOI/JCEOI/SOI system established. The controlling authority for the CEOI/JCEOI/SOI of a major command should be the commander of that organization or his duly designated representative.

9. For locally generated key in electronic form, the organization that directed the key generation performs the controlling authority functions unless those functions are specifically delegated to another organization.

10. The Joint Staff, the commanders of the Unified and Specified Commands, the heads of departments and agencies, or their designees may direct a change in controlling authorities under their command. All cryptonet members, appropriate distribution authorities, and NSA [redacted] must be notified of all controlling authority designations and changes.

SECTION VI - NSA RESPONSIBILITIES

11. NSA is responsible for:

a. Performing controlling authority functions for specified material including, but not limited to, all FIREFLY keying material generated by NSA facilities.

b. Taking or recommending appropriate action when COMSEC material has been subjected to compromise, and notifying appropriate authorities of such actions.

c. When requested, assisting controlling authorities in their annual cryptonet reviews.

d. In coordination with appropriate distribution authorities, advising controlling authorities of the logistic impact of compromise, supersession, or other controlling authority decisions.

SECTION VII - CONTROLLING AUTHORITY RESPONSIBILITIES

12. Cryptonet Management. Controlling authorities direct the establishment and operation of the cryptonet and manage the operational use of material assigned to the cryptonet.

a. Controlling authorities must understand the operational requirements supported by the cryptonet and must be familiar with the operation, capabilities, and doctrinal requirements of the associated equipment or off-line system.

b. For cryptonets using hard copy keying material, controlling authorities will coordinate the establishment and logistic support of the cryptonet by advising appropriate distribution authorities and NSA [redacted] of the COMSEC accounts that are to receive keying material and the number of copies they will receive.

(b)(3)-P.L. 86-36

c. Controlling authorities for off-line cryptosystems must identify specific operational requirements to NSA ( ). Controlling authorities for CEOI/JCEOI/SOI are responsible for updating their requirements to NSA ( ) on a timely basis to permit sufficient lead time for production.

d. Controlling authorities for keying material must specify the initial implementation and supersession dates and inform all cryptonet members, appropriate distribution authorities, and NSA ( ). Controlling authorities for CEOI/JCEOI/SOI are responsible for announcing implementation of the system and informing NSA ( ) of the supersession rate and projected usage to permit timely resupply.

NOTE: Supersession rates (the rates at which the editions are replaced) are established by NSA based on physical and cryptographic security considerations, operational need, and production/resupply constraints. Except in emergencies, controlling authorities will not change supersession rates without proper coordination; for example, a controlling authority will not arbitrarily convert an annually superseded key to a monthly superseded key. However, a controlling authority may extend the effective dates of an edition to make use of spare settings when resupply is uncertain.

e. In situations where material cannot be supplied in time to meet operational requirements, controlling authorities can authorize replacement or resupply of key for machine cryptosystems in accordance with paragraph 16.c. Key encryption key (KEK) must be physically distributed in all but emergency situations, where the alternative is unencrypted communications. Manual cryptosystems (codes, authenticators, and call signs) can be locally reproduced as necessary to meet operational requirements. Controlling authority approval is not required, but material must be issued only to users approved by the controlling authority. Reproduced material must be accounted for in accordance with department or agency directives.

f. If hard copy keying material is being used, controlling authorities must notify all net members, appropriate distribution authorities, and NSA ( ) of any changes in cryptonet structure or keying material status. This includes any changes in keying material effective or supersession dates. If off-line cryptosystems are concerned, controlling authorities must also notify NSA ( ).

g. Controlling authorities will approve classification changes for the key they control. Before upgrading keying material to TOP SECRET, controlling authorities must ensure that it was held under two-person integrity, or that at a minimum, access was restricted to COMSEC account personnel. Controlling authorities must inform NSA ([redacted]) of any classification changes. If off-line systems are used, controlling authorities must also notify NSA ([redacted]).

h. Controlling authorities must maintain accurate records on pertinent aspects of the cryptonet in sufficient detail to manage the membership of the cryptonet and assess the impact of, and to recover from, a compromise. Controlling authority records must show the identity and validate the membership of all cryptonet members, the amount of material each is authorized to hold, the distribution authorities that support the cryptonet, and the most expeditious ways of promulgating supersession and other emergency information to all cryptonet members.

i. Controlling authorities will contact cryptonet members at least annually. At a minimum, controlling authorities will identify the material they control and advise net members how to contact them under normal and emergency circumstances. Controlling authorities are authorized to communicate directly with cryptonet members.

13. Cryptoperiod Extensions. A cryptoperiod is the length of time each setting is authorized for use. Cryptoperiod should not be confused with effective period, which is the length of time an edition is authorized for use. Extending the effective period of an edition to make use of spare key settings is not considered extending the cryptoperiod, but is the prerogative of the controlling authority. Controlling authorities who extend cryptoperiods for reasons other than logistic necessity should follow the guidelines contained in the Annex prior to implementing the extension.

a. When operational requirements necessitate, controlling authorities can extend the cryptoperiod of manual cryptosystems up to 72 hours and auto-manual and machine cryptosystems up to one week, unless the specific cryptosystem doctrine prohibits cryptoperiod extensions or authorizes longer extensions. In cases of conflict, cryptosystem doctrine takes precedence. This authorization applies to both hard copy and locally generated key in electronic form. Controlling authorities for CEOI/JCEOI/SOI may authorize extensions of the

(b)(3)-P.L. 86-36

effective period to suit operational conditions. Controlling authorities are not required to report these extensions to NSA. Net members can extend cryptoperiods up to two hours to complete a transmission or conversation in progress at key change (HJ) time. Controlling authority approval is not required and net members are not required to report these extensions.

b. When user accounts have only two editions of future key remaining, the controlling authority must promptly ascertain the status of follow-on material. If net members cannot be ensured of resupply before their remaining key is expended, the controlling authority must extend the cryptoperiod in accordance with paragraph 13.a. If the extension is insufficient, or a resupply date cannot be determined, controlling authorities must report at IMMEDIATE precedence to NSA (and), who will provide additional instructions. The message must include the short title, number of net members, and explain the necessity for the cryptoperiod extension.

NOTE: When time is of the essence, controlling authorities can verbally request cryptoperiod extensions from NSA . Outside of normal duty hours, controlling authorities should call the NSA . When authorization is given verbally, controlling authorities must take immediate action, and not wait for message documentation. Net members must abide by all verbal instructions relayed by the controlling authority.

14. COMSEC Incidents.

a. Controlling authorities must ensure that, when the keying material is used by members of more than one department or agency, cryptonet members know how to address COMSEC incident reports. Incidents involving CEOI/JCEOI/SOI are not reportable to NSA.

b. Controlling authority responsibilities regarding COMSEC incidents are limited to initiating precautionary supersession or other recovery actions when warranted and rendering an evaluation as part of the administrative closure. Related items such as recommending procedural changes or disciplinary action are outside of the controlling authority's purview.

15. Incident Evaluation. Controlling authorities will evaluate physical COMSEC incidents as specified in NSTISSI No. 4003. Controlling authorities must inform appropriate COMSEC

incident monitoring activities and NSA [redacted] of all evaluations. Controlling authorities for CEOI/JCEOI/SOI will evaluate incidents as specified in department or agency directives.

16. Compromise Recovery. Compromise recovery and incident evaluation are two separate, distinct actions that are required of a controlling authority. Where substantial evidence exists that COMSEC material has been compromised, controlling authorities must take immediate action. Controlling authorities will not wait for incident reporting and evaluating requirements to be satisfied, but will initiate recovery action as soon as they have enough information to make an informed decision. Ideally, controlling authorities will announce precautionary supersession. In the event of compromise of CEOI/JCEOI/SOI, controlling authorities will handle the situation in accordance with department or agency directives.

a. 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. Emergency supersession of hard copy key must be reported immediately to appropriate distribution authorities and NSA ([redacted] and [redacted]) so that resupply action may be taken, replacement material may be produced, and status documents corrected. Emergency supersession of CEOI/JCEOI/SOI must be reported to NSA ([redacted]) to ensure adequate and timely resupply.

b. Superseding locally generated electronic key can present a unique problem for mobile/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.

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

(1) Key may be electronically generated and transmitted to net members via an uncompromised cryptosystem approved for over-the-air key transfer.

(2) Printed key settings may be transmitted by a cryptosystem that provides end-to-end encryption equal to the classification of the transmitted key (e.g., the Automatic Digital Network (AUTODIN) system, secure facsimile, or secure telephone). Printed key settings can also be encrypted by auto-manual or one-time pad system and transmitted over a system that is secured at a lower level than the encrypted key.

(3) Printed key settings may be reproduced and physically transferred to net members. Punched tape will not be reproduced without the authorization of NSA ( ). Converting hard copy keying material to electronic form for equipment fill is not considered reproduction.

(4) Key may be physically transferred to net members in a common fill device or other approved transfer device. When keyed, the common fill device must be protected at the same level as the key it contains.

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

(1) Extend the cryptoperiod of uncompromised keying material in accordance with doctrinal constraints.

(2) Exclude from net operations those members who do not hold or cannot be furnished replacement material.

(3) Suspend cryptonet operations until key can be resupplied.

(4) Continue to use the compromised key. This action is a last resort when normal supersession of the compromised material will take place before emergency supersession can be accomplished, or where keying material changes have a serious detrimental effect on operations, or where no replacement material is available. The controlling authority must alert net members (by other secure means if available) that a possible compromise has taken place and direct that members minimize transmissions using the compromised key. (Use this option only when continued cryptonet operation is absolutely essential to the mission.)

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

17. Annual Reviews. Controlling authorities will initiate periodic reviews of keying material in accordance with the following criteria:

a. Controlling authorities will conduct an annual review of keying material used with machine cryptosystems. Annual reviews must confirm cryptonet structure, membership, quantities and adequacy of key to meet operational requirements, and continuing requirement for the key. The cryptonet must be deactivated if no longer needed. During the review, controlling authorities must identify large cryptosystems of low peacetime use that are candidates for placement into contingency status (see paragraph 18.g, below). A summary of each review must be sent to NSA ( ) and the appropriate distribution authorities.

b. Controlling authorities will review keying material used with off-line cryptosystems and participate in surveys and reviews in accordance with NACSI No. 4007.

c. Controlling authorities will recommend changes in keying material content and format to NSA ( ), and in the case of off-line cryptosystems and CEOI/JCEOI/SOI, to NSA ( ).

18. Other Functions.

a. Controlling authorities will designate keying material to be used for encryption of sensitive compartmented information (SCI).

b. When a controlling authority is notified that a department or agency has granted a waiver to two-person integrity requirements for keying material, the controlling authority will determine if it is appropriate to notify any or all of the other net members.

c. Controlling authorities will specify HJ time for the cryptonet when the time is not prescribed in the keying material. The time selected for HJ must have the least operational impact. Controlling authorities may change HJ time by notifying the net members.

d. Controlling authorities will make spare group assignments of operations codes, as necessary.

e. In fixed telecommunications facilities, controlling authorities will approve the number of extracts of keying material that may be issued to a user at any one time, except where specified in the material. Protectively

packaged keying material should be issued as entire editions whenever possible. Removing key from its protective packaging defeats the purpose of protective packaging and exposes the key to surreptitious copying.

f. In tactical situations, keying material will be issued in sufficient quantities to support mission requirements. Keying material can be issued in either hard copy or electronic form depending on the risk as determined by the local commander. In high risk environments, key will be issued in electronic form. Any multiple key storage capacity of the equipment should be used. If equipment does not have multiple fill capacity, or has insufficient capacity, common fill or approved key transfer devices should be issued. If hard copy keying material is issued, extracts may be issued when only a few settings are required; otherwise the entire edition should be issued. The decision of whether to issue extracts or entire editions should be based on a risk assessment and careful consideration of the logistic problems associated with emergency resupply due to compromise.

g. When large amounts of keying material are provided for regular consumption, and are destroyed unused, the controlling authority should consider placing the material into contingency status. Contingency keying material is keying material slated for a specific, yet irregularly occurring, requirement. The material is not activated until needed for the specific requirement, and is not destroyed until after use. Substantial savings in production, distribution, accounting, and destruction are realized when contingency materials are used in place of regularly superseded effective key. Any action to establish a contingency cryptonet must be coordinated with appropriate distribution authorities and NSA [redacted].

Encl:

Annex - Guidelines for Extending Cryptoperiods

(b)(3)-P.L. 86-36

ANNEX

GUIDELINES FOR EXTENDING CRYPTOPERIODS

1. When cryptoperiods must be extended for reasons other than logistic necessity (e.g., under pre-strike, battlefield, or field training conditions), controlling authorities are strongly 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 the cryptoperiod will be extended.

a. Size of the Cryptonet. Key used on a large cryptonet is usually more vulnerable to compromise than 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 considerably more intelligence available to an adversary. (It is for these reasons that controlling authorities should keep their cryptonets as small as operationally feasible.)

b. Location and Operating Environment of Net Members. Net members located in the United States, its territories, and its protectorates are usually considered to be at less risk than those in other locations. Net members located in a high risk environment (e.g., in an area outside the United States where there is a small or no U.S. 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 do fixed plant net members. In addition, loss on the battlefield could pose an immediate threat not only to U.S. communications but also to U.S. lives.

c. Sensitivity and Perishability of Traffic. The controlling authority should consider the classification of the information being protected, but also whether the information is of long or short-term intelligence value. Compromise of a key used to secure upper echelon strategic communications would have a more devastating effect on U.S. security than would compromise of a key used to secure highly perishable or lower echelon tactical communications. (It is for this reason that "top to bottom" key distribution should be avoided whenever possible.)

d. Emergency Supersession Plan. The controlling authority should have a plan for replacing compromised key. He or she should know approximately how quickly the key can be

replaced and if the plan is realistic in a worst case scenario. It is recommended the controlling authority test the plan, because it is extremely difficult to accomplish an unscheduled rekey in a large net without creating additional problems and confusion. It is essential that the controlling authority know the logistic channels that support the cryptonet as well as the electronic key transfer or distribution capabilities of the associated equipment.

e. Operational Impact of an Extended Cryptoperiod. The controlling authority should make an honest assessment as to whether the cryptoperiod is being extended out of operational necessity or for operator convenience. Although loss of (or the risk of losing) critical communications under battlefield conditions is intolerable, our peacetime training is to prepare us for wartime. If we do not follow standard procedure during wartime, the value of our peacetime training is questionable. Also, feedback from personnel involved in recent military operations has revealed that operators were confused by changes in operational procedures during the stress of a wartime environment.

2. If cryptoperiod extensions are necessary to maintain critical communications during battle (actual or training), the following guidelines should be followed:

a. All preplanned cryptoperiod extensions should begin with a new key setting.

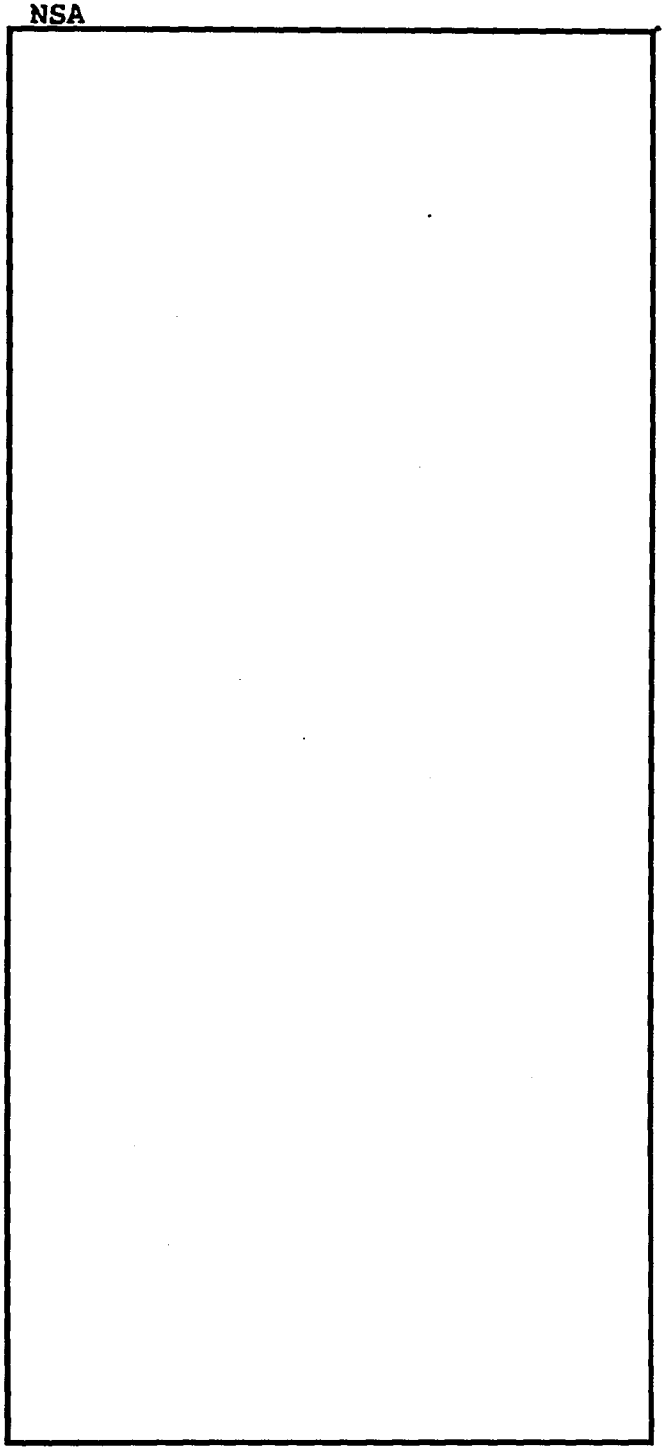
b. Whenever possible, cryptoperiods should be extended by net and not by short title.

c. All affected nets should be directed to rekey as soon as there is a break in activity.

NSTISSI No. 4006

(b)(3)-P.L. 86-36

DISTRIBUTION:
NSA



~~FOR OFFICIAL USE ONLY~~

(b)(3)-P.L. 86-36