~~CONFIDENTIAL~~

NSTISSI No. 3017
August 1996
Revised March 2003

NSTISS

NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE FOR NON-TRI-TAC KG-84A, KG-84C, KIV-7, KIV-7HS, KIV-7HSA, AND KIV-7HSB (U)

THIS DOCUMENT PROVIDES MINIMUM STANDARDS, FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY

~~CONFIDENTIAL~~

Derived Fr: NSA/CSSM 123.2
dtd 3 Sep 91
Declass On: Source marked OADR
Date of source: 3 Sep 91

NSTISS

NATIONAL SECURITY
TELECOMMUNICATIONS
AND INFORMATION
SYSTEMS SECURITY

NATIONAL MANAGER

FOREWORD

1. (U) This National Security Telecommunications and Information Systems Security Instruction (NSTISSI) provides security doctrine for the KG-84A in non-TRI-TAC applications and for the KG-84C, KIV-7, KIV-7HS (high-speed), KIV-7HSA, and KIV-7HSB COMSEC equipment. Operational security for the TRI-TAC system has been published separately.

2. (U) This document is effective upon receipt and supersedes NSTISS No. 3017, Operational Security Doctrine for Stand-Alone KG-84, KG-84A, and KG-84C, dated 21 September 1991. (With the replacement of the KG-84 by KG-84A in the TRI-TAC System, the need for an operational security doctrine covering the KG-84 no longer exists.)

3. (U) Extracts from this document may be made for official purposes. Extracts of paragraphs 19, 19.1, and/or 19.2 must be marked CONFIDENTIAL. Extracts of other paragraphs must be marked FOR OFFICIAL USE ONLY.

4. (U) Representatives of the NSTISS Committee may obtain additional copies of this instruction from:

NSTISSC SECRETARIAT
ATTN: [redacted] (b)(3)-P.L. 86-36
NATIONAL SECURITY AGENCY
9800 SAVAGE RD STE 6716
Ft MEADE MD 20755-6716

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

KENNETH A. MINIHAN
Lieutenant General, USAF

NSTISSI No. 3017
Revised March 2003

OPERATIONAL SECURITY DOCTRINE FOR NON-TRI-TAC KG-84A, KG-84C, KIV-7, KIV-7HS, KIV-7HSA, AND KIV-7HSB (U)

SECTION I - INTRODUCTION (U)

1. (U) **Purpose.** This document contains minimum security standards for safeguarding, controlling, and using the KG-84A/C and KIV-7/7HS communications security (COMSEC) systems. The COMSEC material comprising these systems is listed in ANNEX A.

NOTE: (U) Since KG-84s have been removed from the U.S. COMSEC inventory, "KG-84" is used throughout the remainder of this document to mean "KG-84A" and/or "KG-84C." *Distinction between these equipment types is made only when necessary.*

NOTE: (U) Throughout the remainder of this document, the KIV-7, KIV-7HS (high-speed), KIV-7HSA, and KIV-7HSB equipment is referred to as "KIV-7." Distinction between these equipment types is made only when necessary.

2. (U) **Application.** The information contained in this document is applicable to U.S. Government departments, agencies, and contractors who handle, distribute, account for, store, or use KG-84 and/or KIV-7 COMSEC equipment and associated COMSEC material.

3. (U) **Waivers.** Requests for waivers of the provisions of this documentmust be submitted through appropriate information systems security (INFOSEC) channels to the NSTISSC Sectretariat.

4. (U) **Promulgation.** Departments and agencies of the Federal Government are obligated to disseminate the information in this document to their subordinate elements and contractors who use the KG-84 or KIV-7 systems. Promulgation may be effected by issuing this document or by incorporating its contents in department/agency publications.

5. (U) **Relationship to Other Documents**

5.1 (U) **Unkeyed Controlled Cryptographic Item (CCI).** NSTISSI No. 4001 states the minimum requirements for controlling unkeyed CCI equipment and components.

5.2 (U) **Keyed CCI.** NACSI No. 4005 states the minimum standards for safeguarding and controlling keying materials and keyed CCI equipment and devices.

5.3 (U) **TOP SECRET Key.** NTISSI No. 4005 states the minimum standards for safeguarding and controlling KG-84 and KIV-7 key that is classified TOP SECRET.

5.4 (U) Terminal Facilities. NACSI No. 4008 states the minimum standards for safeguarding COMSEC facilities.

5.5 (U) Maintenance. NSTISSI No. 4000 states minimum standards, delineates responsibilities, and establishes procedures for COMSEC equipment maintenance and maintenance training.

5.6 (U) TEMPEST. NSTISSI No. 7000 states guidelines, restrictions, and procedures for applying TEMPEST countermeasures for equipment, systems, and facilities that process national security information.

5.7 (U) Installation. NSTISSAM TEMPEST 2/95 states minimum security-related engineering guidelines for establishing adequate installation of systems that process such information.

5.8 (U) Protected Distribution Systems. In fixed-plant KG-84 and KIV-7 applications, cables connecting printers and other terminal equipment to the COMSEC equipment must meet the provisions of NACSI No. 4009.

5.9 (U) Controlling Authorities. Responsibilities and prerogatives of controlling authorities (CAs) for COMSEC keying material are stated in NSTISSI No. 4006.

6. (U) Conflict with Other Documents. In case of conflict between the provisions of this and other national-level documents, this document takes precedence in matters relating to the KG-84 and KIV-7 systems. However, such conflicts should be brought to the attention of the NSA INFOSEC Policy and Doctrine Division.

7. (U) References. ANNEX B lists the documents that are referenced in this instruction.

8. (U) Definitions. NSTISSI NO. 4009 applies to this document. The following definitions also apply:

8.1 (U) COMSEC Emergency - Operational situation, as perceived by the responsible commander, in which the alternative to strict compliance with procedural restrictions affecting use of COMSEC equipment would be plain text communications.

NOTE: (U) As used in this definition, the term "responsible commander" includes equivalent civil agency officials.

8.2 (U) Electronic Key - Encrypted or unencrypted key in electronic form that is stored on magnetic media or in electronic memory, transferred by electronic circuitry, or loaded into COMSEC equipment.

8.3 (U) Sequential OTAR - Electronically replacing the traffic encryption key in remote COMSEC equipment associated with a multi-station net, one terminal at a time.

8.4 (U) Simultaneous OTAR - Electronically replacing the traffic encryption key in remote COMSEC equipment associated with a multi-station net, all at the same time.

8.5 (U) Strategic Traffic - Information having high sensitivity and/or long-term intelligence value.

8.6 (U) Tactical Traffic - Information having low sensitivity and/or short-term intelligence value.

SECTION II - EQUIPMENT DESCRIPTION (U)

9. (U) **Equipment Types.** The cryptographically compatible KG-84 and KIV-7 COMSEC equipment is capable of operating in the full-duplex, half-duplex, and simplex (broadcast) modes. They provide cryptographic security for digital point-to-point circuits and multi-station nets that transmit teletypewriter and data traffic, including digitalized voice.

NOTE: (U) KG-84s can encrypt and decrypt synchronous traffic at rates up to 64 kilobits per second (Kbps) and asynchronous data rates from 1 to 9.6 kbps. KIV-7s accept synchronous data up to 512 Kbps and asynchronous data up to 288 Kbps. KIV-7HS equipment accepts data up to 1.544 megabits per second and asynchronous data up to 288 Kbps)

9.1 (U) **KG-84A.** The KG-84A was designed for use on landline, microwave, and satellite nets and circuits.

9.2 (U) **KG-84C.** The KG-84C is operationally similar to the KG-84A, but has enhanced synchronization modes that permit it to operate effectively in high frequency radio applications and on European TELEX circuits.

9.3 (U) **KIV-7.** The KIV-7 is an embeddable COMSEC module that is functionally similar to the KG-84 in most modes of operation. It may be plugged into a variety of terminals, such as personal computers, workstations, and facsimile equipment, or used as a stand-alone equipment to secure data communications. Through use of the KIV-7 integrated remote control interface, net control stations (NCSs) or "master stations" can manage and rekey up to 30 "slave stations" or outstations (OSs)

CAUTION: (U) KIV-7 master units perform only remote control functions, and slave units perform only communications functions. Internal strapping for master and slave KIV-7s is preset at the factory and noted on the equipment label. Do not open the KIV-7 to change these straps, since opening a KIV-7 voids its warranty.

NOTE: (U) The KIV-7 supports both Data Standard 101 (AN/CYZ-10) and data Data Standard 102 (KOI-18, KYK-13 and KYX-15).

10. (U) **Security of Traffic.** When appropriately keyed, KG-84s and KIV-7s are approved for securing information of all classifications and categories.

11. (U) **Keying Related Functions.** KG-84s and KIV-7s are capable of the following keying related functions:

11.1 (U) **Non-OTAR Key Loading.** KG-84 and KIV-7 secured nets/circuits may operate using only traffic encryption key (TEK) that is loaded locally at each terminal.

11.2 (U) **TEK Update.** Use of the KG-84 and KIV-7 capability to locally update installed traffic encryption key is appropriate when over-the-air rekeying (OTAR) is not used to change installed TEK.

11.3 (U) **Point-to-Point OTAR.** In their manual rekeying (MK) mode, KG-84 and KIV-7 equipment can immediately replace installed TEK on point-to-point circuits via OTAR.

NOTE: (U) KG-84 and KIV-7 MK is a "non-cooperative" process, in that it requires no operator actions at the receiving terminal(s).

11.4 (U) **Net OTAR.** In their automatic rekeying (AK) mode, the KG-84 and KIV-7 equipment can immediately replace installed TEK on multi-station nets via OTAR. If more than one key encryption key (KEK) is used in a multi-station net, OTAR must be accomplished by the longer, sequential OTAR method. However, if a common KEK or a start-up KEK is used, the shorter, simultaneous OTAR method can be used.

NOTE: (U) KG-84 and KIV-7 AK is also "non-cooperative."

11.5 (U) OTAT. Using their manual rekeying/receive key (MK/RV) mode, KG-84 and KIV-7 equipment can transfer 128-bit key via over-the-air key transfer (OTAT). Key thus transmitted may be extracted from a receiving terminal and used to key other COMSEC equipment. KEK assignment determines whether OTAT is sequential or simultaneous.

NOTE: (U) KG-84 and KIV-7 OTAT is a "cooperative" process, in that it requires action by receiving terminal operators.

11.6 (U) KIV-7 Remote Key Change. In applications for the KIV-7 only that are configured for remote control, OS (slave station) operators may load the next-up TEK ahead of time into an "X" fill register other than the one containing the active TEK, and the NCS (master) station operator can activate the new TEK remotely.

SECTION III - KEYING (U)

12. (U) Types of Key. In KG-84 only applications and in mixed KG-84/KIV-7 applications, the COMSEC equipment may use either non-OTAR TEK exclusively or KEK (or start-up KEK) to replace TEK via OTAR. These options are also available to NCSs of nets/ circuits that are secured only by KIV-7s that are not configured for remote control of the OSs. However, in KIV-7 only applications that are configured for remote control, the master KIV-7 uses remote control TEK (RCTEK) to secure OS control and status functions and remote control KEK (RCKEK) to secure TEK replacement in OSs.

NOTE: (U) The KIV-7 also uses a physical crypto-ignition key (CIK) nomenclatured "DK1024" to prevent unauthorized access to internally stored key and to "unlock" the equipment for secure operation.

12.1 (U) TEK is used to secure the information that is transmitted on KG-84 and KIV-7 secured nets/circuits. KG-84/KIV-7 TEK should be referred to as either "OTAR TEK" or "non-OTAR TEK."

12.1.1 (U) Sources of TEK. KG-84 and KIV-7 non-OTAR TEK normally originates as NSA-produced, punched paper tape. However, OTAR TEK may be generated by/for the NCS by a certified key variable generator (KVG), such as a KG-83 or KGX-93/93A. Whenever it is operationally feasible to do so, OTAR TEK should be field generated. This can be done by acquiring a certified KVG or by taking an AN/CYZ-10 to a certified KVG and filling it with up to 1,000 128-bit keys.

NOTE: (U) Any NCS that performs 50 or more OTAR operations per week should requisition a KG-83 (with single-equipment mounting tray) to generate OTAR TEK. This obviates the resupply of and accounting for punched tape TEK.

12.1.2 (U) TEK Distribution. KG-84 and KIV-7 TEK may be distributed physically, in tape form or in keyed fill devices, or electronically, via OTAR or OTAT. When it is operationally feasible to do so, TEK should be distributed electronically.

12.1.3 (U) TEK Allocation. Separate TEK must be used for each KG-84 and KIV-7 net or circuit. Collections of independent point-to-point circuits that hub at the same NCS must not be keyed as "nets."

NOTE: (U) Whether an NCS operates a net (that uses common TEK for all associated OSs) or a collection of point-to-point circuits (each of which uses unique TEK) depends on whether the OSs intercommunicate directly, as occurs in radio nets, or through a switch located at the NCS. Dial-up circuits, where the NCS uses a single KG-84 or KIV-7 to communicate with all of the OSs, one at a time, must be keyed as "nets."

12.1.4 (U) TEK Cryptoperiods. KG-84 and KIV-7 TEK cryptoperiods are based on such factors as whether the application is a point-to-point (P-T-P) circuit or multi-station net, whether the net/circuit serves a strategic (fixed-plant) or tactical purpose, whether the net/circuit distributes key physically or via OTAR, whether the using net/circuit operates full-time or part-time, and whether the net/circuit is authorized to transmit classified or only unclassified data. Doctrine for selecting the appropriate cryptoperiod is stated below:

12.1.4.1 (U) Full-time Nets/Circuits. KG-84 and KIV-7 secured nets and circuits that operate continuously may terminate in spaces that are continuously manned by appropriately cleared persons; in unmanned spaces that meet Service, department, or agency standards for open storage of classified information at the level of the TEK used; or in drilled security containers approved by the General Services Administration or NSA for storage of keyed COMSEC equipment.

NOTE: (U) In this document, tactical nets/circuits that operate continuously while they are needed to support an operation or exercise but that close down when they are no longer needed are categorized as full-time nets/circuits.

12.1.4.2 (U) Classified, Fixed-plant, Full-time Nets & Circuits. Authorized cryptoperiods for TEK used with non-tactical, KG-84 and KIV-7 secured nets/circuits that operate continuously and are authorized to transmit classified information are shown in the following chart.

OTAR	NON-OTAR	FULL TIME	PART TIME	AUTHORIZED CRYPTOPERIODS
X		X		Week
X			X	Day with OTAR at close of business each work day
	X	X		Day or Month with update at COB each work day
	X		X	Day (Zeroize at close of business each work day)
				Month with update at close of business each work day

12.1.4.2.1 (U) Unclassified, Fixed-Plant, Full-time Nets & Circuits. The maximum cryptoperiod for TEK used with non-tactical, KG-84 and KIV-7 secured nets/circuits that operate continuously and are not authorized to transmit classified information is one month without updating or OTARing.

12.1.4.2.2 (U) OTARing Tactical Full-time Nets and Circuits. The maximum cryptoperiod authorized for OTAR TEK used with tactical KG-84 and KIV-7 circuits that operate continuously while they are active is one week.

12.1.4.2.3 (U) Non-OTARing Tactical Full-time Nets and Circuits. The maximum cryptoperiod authorized for non-OTAR TEK used on tactical KG-84 and KIV-7 secured nets/circuits that operate continuously when they are active is one month. with update on each day the net/circuit is active.

NOTE: (U) In some tactical applications it is necessary for mobile users to leave and reenter KG-84 and KIV-7 nets/circuits, often more than once during individual cryptoperiods. Because of the high vulnerability of exposed key tape segments and key stored in KYK-13 and KYX-15 fill devices, operational requirements to retain KG-84 and KIV-7 TEK for use later in a cryptoperiod should be accommodated by use of redundant segment tape formats, such as the "DC" (5 copies each of 6 unique keys - monthly cryptoperiod). After extracting it from its canister, a user may retain the last redundant tape segment of such TEK until it is superseded, but this easement does not apply to tape segments from short titles that are not produced in one of the redundant formats.

12.1.4.2.4 (U) Part-time Nets & Circuits. The cryptoperiod for TEK used on nets or circuits that close down for predetermined periods (e.g., at night or on weekends) and that are secured either by KG-84s only or mixes of KG-84s and KIV-7s is one day. Daily key changes may be accomplished by OTAR at (or near) the end of activity on each day the net/circuit is active; by loading monthly cryptoperiod, non-OTAR TEK and updating it locally at net or circuit close-down; or by loading a new segment of non-OTAR TEK at the start of net/circuit activity on each working day and zeroizing the COMSEC equipment at each net or circuit close-down. Where it is operationally feasible to do so, TEK used for part-time, KG-84 and KG-84/KIV-7 secured net and circuits should be changed via OTAR.

12.1.4.2.5 (U) Part-time KIV-7 Only Secured Nets and Circuits. The maximum cryptoperiod authorized for TEK used on fixed-plant, part-time nets/ circuits secured exclusively by KIV-7s is one week, month, but the CIK must be extracted and stored at the end of each net/circuit working day.

12.1.4.3 (U) Cryptoperiod Extensions. The controlling authority or NCS of any full-time KG-84 or KIV-7 secured net or circuit may extend its TEK cryptoperiod for up to seven days without report. Longer extensions must have prior NSA approval or be reported as COMSEC incidents.

12.1.5 (U) Routine Key Supersession. There is no relationship between the routine supersession of OTAR TEK and OTAR KEK or start-up KEK. When a new KEK or start-up KEK is installed, the TEK in use should be retained and not zeroized. i.e., a cold start is not required each time a KEK is replaced.

12.1.5.1 (U) TEK Classification. Except in COMSEC emergencies, TEK must be classified at the level of the highest classified information that is normally transmitted on the net/circuit with which it is used.

12.1.5.2 (U) Tape OTAR TEK Classification. In applications where one short title of key tape serves as the source of OTAR TEK for several nets/circuits, it must be classified at the level of the highest classified information any of the nets/circuits is authorized to transmit. As each segment is used, it is notionally downgraded to the level of the net or circuit on which it is used, but need not be physically remarked to reflect such downgrading.

12.1.6 (U) Electronic OTAR TEK Classification. A certified KVG may generate KG-84/KIV-7 TEK at any classification. Each electronic key extracted from a KVG must be assigned a classification by the user in whose fill device it is stored.

12.1.7 (U) Loading TEK. Electronic key may be loaded into KG-84s and KIV-7s locally from AN/CYZ-10, KYK-13, or KYX-15 fill devices, and tape key may be loaded from KOI-18s.

12.1.7.1 (U) Cold Starting.

12.1.7.1.1 (U) OTAR Cold Starting. NCS and OS operators of unkeyed KG-84s and KIV-7s used with nets and circuits that rekey via OTAR must initialize their equipment by loading the appropriate segment of KEK or start-up KEK into both the "U" (KEK) fill register and an "X" (TEK) fill register and then **updating the key in the "X" register**. (This is a new procedural step that may not yet be included in operating instructions.) The NCS must then immediately replace the key in the "X" register via OTAR.

12.1.7.1.2 (U) KG-84 Non-OTAR Cold Starting. Operators of unkeyed KG-84s used with nets and circuits that do not rekey via OTAR must load the next-up (or designated) segment of TEK directly into an "X" fill register of their equipment, except that when a KG-84 terminal space is continuously manned by personnel who are cleared to the level of the TEK, non-OTAR TEK may be loaded into the KG-84 "V" register and transferred to an "X" register at key change time.

CAUTION: (U) Use of the KG-84 "fill V" key loading routine is prohibited at terminals that are *not continuously manned* by properly cleared personnel.

NOTE: (U) The above limitation on use of "fill V" does not apply to the KIV-7.

12.1.7.2 (U) Rekeying

12.1.7.2.1 (U) Rekeying Full-time Nets and Circuits. TEK for KG-84 and/or KIV-7 secured, full-time nets and circuits that distribute TEK via OTAR may be changed at any time chosen by the NCS.

12.1.7.2.2 (U) Rekeying Part-time Nets and Circuits.

12.1.7.2.2.1 (U) KG-84 OTAR. TEK for part-time nets/circuits that distribute TEK via OTAR and are secured by all KG-84s or mixes of KG-84s and KIV-7s *must be changed* at (or near) close of business on each day the net or circuit is active.

NOTE: (U) KG-84 terminals of part-time nets and circuits may then be left keyed and unmanned until the net/circuit is reactivated, provided the terminal space is locked and the door key is controlled and such other physical security safeguards as the local commander may prescribe are enforced.

12.1.7.2.2.2 (U) KIV-7 OTAR. TEK for part-time nets/circuits that are secured only by KIV-7s and that distribute TEK via OTAR must be changed at (or near) close of business on each day the net or circuit is active. However, if an NCS instructs all OSs to remove and secure their CIKs at net/circuit close-down, the net/circuit may be rekeyed as if it were a full-time net/circuit, i.e., OTAR TEK may be replaced at weekly intervals.

12.1.7.2.3 (U) Non-OTAR Rekeying.

12.1.7.2.3.1 (U) Part-time Manned Terminal Spaces. For part-time KG-84 and KIV-7 secured nets and circuits that are not rekeyed via OTAR, operators may load non-OTAR TEK for the next cryptoperiod into a vacant "X" fill register at any time during the preceding cryptoperiod.

CAUTION: (U) Use of the "fill V" loading routine at KG-84A/C secured, part-time manned terminal spaces is prohibited, but this prohibition does not apply to KIV-7 secured part-time nets/circuits.

12.1.7.2.3.2 (U) Manned Terminal Spaces. If a KG-84 terminal space is continuously manned by personnel who are cleared at least to the level of the TEK, the operator may load the next-up non-OTAR TEK into the "V" register and perform a V-to-X transfer at key change time.

12.2 (U) KEK. KEK is used to secure TEK during electronic distribution.

12.2.1 (U) Sources of KEK. KG-84 and KIV-7 KEK normally originates as punched tape; however, when delivery to all users can be accomplished physically, through distribution of keyed fill devices, KEK may also be field-generated by certified KVGs.

NOTE: (U) Where KEK in electronic form can be delivered physically to all users, as might be the case when all users of a local message delivery complex receive key from the same COMSEC account, it may not be necessary to use tape KEK. Acceptable alternatives are to field-generate KEK with a certified KVG or to dedicate segments of a OTAR TEK tape for use as the local net KEKs. In either case, local distribution of the KEK would be made by means of keyed fill devices.

12.2.2 (U) KEK Distribution. Except in COMSEC emergencies, KG-84 and KIV-7 KEK must be distributed physically, in punched tape form or in keyed fill devices.

NOTE: (U) In COMSEC emergencies, such as when it becomes necessary to add a new terminal to an existing tactical net, individual segments of KEK may be distributed via OTAT, on nets/circuits that are secured by KG-84 and KIV-7 equipment.

12.2.3 (U) KEK Allocation. For KG-84 and KIV-7 secured nets and circuits that distribute TEK via OTAR, have stable composition, and exist on a continuing basis, designated KEK should be used instead of start-up KEK.

12.2.3.1 (U) Point-to-Point Circuits. A separate KEK must be used for each KG-84 or KIV-7 secured circuit.

NOTE: (U) In situations where parallel circuits terminate in the same spaces at both terminals, separate segments from a single short title of tape KEK may be used.

12.2.3.2 (U) Multi-station Nets. One or more separate KEK must be used with each KG-84 or KIV-7 secured net. NCSs may assign the same KEK to all net members, as a basis for performing simultaneous OTAR; may assign a separate KEK to each net OS, as a basis for performing sequential OTAR; or may combine the two practices, so that some OSs hold unique KEK and others hold KEK in common.

12.2.4 (U) KEK Cryptoperiods.

12.2.4.1 (U) Maximum Cryptoperiods. The maximum cryptoperiod authorized for each KG-84 and KIV-7 KEK is three months.

NOTE: (U) Continued use, throughout its authorized three-month cryptoperiod, of a tape KEK segment drawn from an edition that is superseded after the cryptoperiod starts is not a reportable COMSEC incident.

12.2.4.2 (U) Extensions. CAs may extend KG-84 and KIV-7 KEK cryptoperiods for up to seven days. Longer extensions must have prior NSA approval or be reported as COMSEC incidents.

12.2.5 (U) U) KEK Classification. KEK must be classified at the level of the highest classified TEK it is authorized to secure.

12.2.6 (U) KEK Updating. As part of each OTAR or OTAT cycle, KG-84 and KIV-7 OSs and the NCSs on point-to-point circuits automatically update their KEKs. In netted applications KEK installed in KG-84 and KIV-7 NCS terminals must be updated manually after each OTAR/OTAT action.

CAUTION: (U) KG-84 and KIV-7 KEK must not be updated more than 99 times.

12.2.7 (U) KEK Storage Capability. Each KG-84 and KIV-7 can store one KEK at a time in its "U" register.

NOTE: (U) The NCS for each KG-84 and KIV-7 secured net that distributes TEK via OTAR must store all OS KEKs in an AN/CYZ-10 or KYX-15 between OTAR cycles.

12.3 (U) Start-up KEK. Start-up KEK is functionally similar to KEK, but is not dedicated to a particular net or circuit. It is used to activate OTAR-capable, tactical nets and circuits that are secured by KYV-5/KY-99/100s, KY-57/58/67s, KG-84A/Cs, or KIV-7s and that do not have designated KEKs. Where it is held in common by a group of potential communicating entities, a start-up KEK may be used to create any number of tactical nets and circuits for their use.

12.3.1 (U) Source of Start-up KEK. Start-up KEK is produced in punched tape form in the "VA" format (one copy each of 62 segments - daily cryptoperiod), and each edition is effective for two consecutive months.

12.3.2 (U) Start-up KEK Distribution. Start-up KEK must be pre-positioned in tape form or converted from tape to electronic form and delivered physically, in keyed fill devices. In COMSEC emergencies, individual segments of start-up KEK may be distributed via OTAT.

12.3.3 (U) Start-up KEK Allocation. The basis for requisitioning a start-up KEK is the potential need of any group of commands or activities to intercommunicate securely on a short-notice basis. The CA for each start-up KEK must designate and maintain records of its holders, must designate its potential NCSs, and must ensure that each designated NCS holds a KYX-15 or AN/CYZ-10 and a source of TEK, such as a KG-83 or a tape TEK.

12.3.4 (U) Start-up KEK Cryptoperiod.

12.3.4.1 (U) Day/Date Relationship. Each segment of start-up KEK becomes effective for one day, on the basis of a predictable day/date relationship.

NOTE: (U) Segments 1A thru 31A are available for establishing nets/circuits during the first month an edition is effective, and segments 1B thru 31B are available for use during the second month.

12.3.4.2 (U) Extensions. The cryptoperiod of start-up KEK may not be extended. If it is necessary to add OSs to a net that was created with start-up KEK, the NCS uses the segment that is effective on the day the additions are made.

12.3.5 (U) Start-up KEK Classification. Except in COMSEC emergencies, start-up KEK must be classified at the level of the highest classified TEK it is intended to secure.

12.4 (U) KIV-7 RCTEK. RCTEK is used in KIV-7 only, remote control applications to secure command and status information transmitted between a NCS (master station) and its OSs (slave stations).

NOTE: (U) RCTEK must be in the Data Standard 74 (256 bit) format; 128 bit key cannot be used.

12.4.1 (U) Source of RCTEK. KIV-7 RCTEK must be centrally produced in punched tape form.

12.4.2 (U) RCTEK Distribution. KIV-7 RCTEK must be distributed physically, as punched tape or in keyed fill devices.

12.4.3 (U) RCTEK Allocation. Each KIV-7 only net must use a unique RCTEK.

12.4.4 (U) RCTEK Cryptoperiod.

12.4.4.1 (U) Maximum Cryptoperiod. The maximum cryptoperiod of KIV-7 RCTEK is three months.

12.4.4.2 (U) Extensions. The CA of KIV-7 RCTEK may extend its cryptoperiod for up to seven days. Longer extensions must have prior NSA authorization or be reported as COMSEC insecurities.

12.4.5 (U) RCTEK Classification. KIV-7 RCTEK must be CONFIDENTIAL when the circuit(s) connecting a master station and its associated slave station(s) pass outside controlled spaces, but may be UNCLASSIFIED when such circuits remain in controlled spaces.

12.4.6 (U) 11.4.6.(U) Loading RCTEK. KIV-7 RCTEK must be loaded locally into the "XRC" fill register.

12.5 (U) KIV-7 RCKEK. RCKEK is used in KIV-7 only, remote control applications to secure TEK that is transmitted from a NCS (master station) to its OSs.

NOTE: (U) RCKEK must be in the Data Standard 74 (256 bit) format; 128 bit key cannot be used.

12.5.1 (U) Source of RCKEK. RCKEK must be produced in punched tape form.

12.5.2 (U) Distribution of RCKEK. KIV-7 RCKEK must be distributed physically, as punched tape or in keyed fill devices.

12.5.3 (U) RCKEK Allocation. Each remote controlled KIV-7 secured net must use a unique RCKEK.

12.5.4 (U) RCKEK Cryptoperiod.

12.5.4.1 (U) Maximum Cryptoperiod. The maximum cryptoperiod of KIV-7 remote control KEK is three months.

12.5.4.2 (U) Extensions. The CA of KIV-7 RCKEK may extend its cryptoperiod for up to seven days. Longer extensions must have prior NSA authorization or be reported as COMSEC insecurities.

12.5.5 (U) RCKEK Classification. KIV-7 RCKEK must be classified CONFIDENTIAL when the circuit(s) connecting the master station to its associated slave stations pass outside controlled spaces, but may be UNCLASSIFIED when such circuit(s) remain in controlled spaces.

12.5.6 (U) Loading RCKEK. KIV-7 RCKEK must be loaded locally into the "W" fill register.

12.6 (U) OTAT Doctrine. KG-84 and KIV-7 equipment is authorized to transmit 128-bit key via OTAT.

12.6.1 (U) Key Loading. When OTAT is performed on a KG-84 or KIV-7 secured net/circuit, every participating COMSEC equipment must hold the same TEK in its active "X" register and the OS(s) that receive an OTAT transmission must hold KEK in common.

12.6.2 (U) Key Tagging. Key transmitted via OTAT on a KG-84 or KIV-7 secured net/circuit must be identified to show its originator, purpose, classification, and effective period. Tags must be passed by separate messages.

12.6.3 (U) Record Keeping. When a key is transmitted via OTAT on a KG-84 or KIV-7 secured net/circuit, the sending, receiving, and relaying stations must keep records of its electronic distribution, at least until the key is superseded.

12.7 (U) Ordering Tape Key. The CA of each new and existing short title of KG-84 and KIV-7 tape key must assign it a long title (up to 100 characters) that identifies its purpose. Sample long titles for the various type of KG-84 and KIV-7 keys are shown in the following table.

SAMPLE KG-84 & KIV-7 KEY TAPE LONG TITLES

PURPOSE	LONG TITLE
KG-84 OTAR KEK	KG-84 Operational OTAR KEK Key Tape
KIV-7 and KG-84 & KIV-7 OTAR KEK	KIV-7 Operational OTAR KEK Key Tape
KG-84 Non-OTAR TEK	KG-84 Operational Non-OTAR Key Tape
KIV-7 and KG-84 & KIV-7 Non-OTAR TEK	KIV-7 Operational Non-OTAR Key Tape
Start-up KEK	Operational Start-up KEK Key Tape
KIV-7 Remote Control TEK	KIV-7 Operational Remote Control TEK Key Tape
KIV-7 Remote Control KEK	KIV-7 Operational Remote Control KEK Key Tape

NOTE: (U) NSA assigns short titles from one series to key intended for use with nets and circuits that are secured exclusively by KG-84s. Short titles from another series are assigned to key intended for use on KIV-7 only nets/circuits and nets/circuits that use mixes of KG-84s and KIV-7s. KIV-7 RCKEKs and RCTEKs are assigned from still another series.

SECTION IV - CRYPTONET SIZE (U)

13. (U) **Limiting Net Size.** KG-84 and KIV-7 cryptonets should be kept as small as possible, to limit the consequences of key compromises and to lessen the problems associated with unscheduled supersessions.

13.1 (U) **TEK Net Size.** Regardless of whether a KG-84 or KIV-7 is field-generated and distributed via OTAR or is centrally produced in tape form and distributed physically, its holders must be limited to commands and activities that have an existing or potential requirement to intercommunicate.

13.2 (U) **KEK Net Size.**

13.2.1 (U) **Point-to-Point KEK Net Size.** Unless there is a compelling operational requirement to do otherwise, only two copies may be ordered for each KEK intended for use with a KG-84 and KIV-7 secured point-to-point circuits.

13.2.2 (U) **Multi-station KEK Net Size.** Only commands and activities that have an existing or potential requirement to inter-communicate may be authorized as holders of KG-84 and KIV-7 secured net KEK; however, CAs may requisition a reasonable number of extra copies to accommodate future net expansion.

NOTE: (U) NSA may challenge tape copy counts of over 50.

13.3 (U) **Start-up KEK Net Size.** Holders of each start-up KEK must be U.S. or allied military commands or civil department or agency activities that have potential need to participate in KY-57/58/67, KYV-5/KY-99/100, KG-84 and/or KIV-7 secured nets or circuits.

NOTE: (U) NSA may challenge requests for production of start-up KEKs having copy counts higher than 250.

13.4 (U) **KIV-7 RCTEK and RCKEK Net Size.** KIV-7 RCTEK and RCKEK net sizes are limited to 31 copies.

SECTION V - RESTRICTIONS (U)

14. (U) **Distributing KEK Electronically.** Except in COMSEC emergencies, KEK and start-up KEK may not be distributed via OTAT.

15. (U) **Key Updating.** KG-84 and KIV-7 TEK, KEK, and Start-up KEK may not be updated more than 99 times.

16. (U) **Fill V.** Except at terminals that are continuously manned by properly cleared persons, TEK may not be loaded locally into the "V" register of KG-84 equipment.

17. (U) **KIV-7 Warranty.** Opening a KIV-7 for any reason voids its warranty.

18. (U) **Printed Garbles.** When the KG-84 is operated in communications mode 5 in a record communications system that produces printed output, printed garbles will appear each time the KG-84 resynchronizes or drops out of synchronization. Pages containing such printed

garbles must be classified at the level of the TEK used. If a message having a classification that is lower than that of the TEK contains such garbles, it must be classified at the level of the TEK. However, if the garbles are deleted, the message may be handled at its normal classification.

19. (U) Use of KG-84 OP2 Mode.

19.1 ~~(C)~~ [redacted]

19.2 ~~(C)~~ [redacted]

20. (U) KIV-7HSA and 7HSB Operational Limitation. The KIV-7HSA and 7HSB must be in the online mode when powered up but not in use. If the KIV-7HSA or 7HSB is left in the offline mode while powered up, the header bypass indicators (light and message display on the front panel, as well as the tone) must be visible and audible to the user.

SECTION VI - CLASSIFICATION, MARKING, AND ACCOUNTABILITY (U)

21. (U) Sources of Guidance. General classification guidance for COMSEC material is contained in NTISSI No. 4002. The classification, marking, and COMSEC Material Control System accountability legend code of each component of the KG-84 and KIV-7 COMSEC system are shown in ANNEX A.

SECTION VII - PHYSICAL SECURITY (U)

22. (U) Safeguarding KIV-7 CIKs. When they are removed from the KIV-7s with which they are associated, CIKs become UNCLASSIFIED CCIs. However, each removed CIK must either be retained in the custody of an authorized user or securely stored at the level of the most highly classified key held in the associated equipment. If a KIV-7 CIK is found installed or unsecured in an unmanned terminal site, the circumstances must be reported as a COMSEC incident.

23. (U) Safeguarding Keyed Equipment and Devices. Security for keyed KG-84 and KIV-7 equipment used in the following applications is summarized below:

23.1 (U) Full-time Manned - Full-time Operated. The security for KG-84 and KIV-7 terminals in this category is ensured by the continuing presence of appropriately cleared operators.

23.2 (U) Part-time Manned - Part-time Operated. In terminal spaces that are manned part-time and in which KG-84 or KIV-7 secured nets/circuits are operated part-time, the COMSEC equipment may be left keyed when the spaces are unmanned, provided the TEK is replaced by either OTAR or updated at the close of business on each working day. Reasonable measures must also be taken to protect the equipment against theft, tampering, or unauthorized use.

NOTE: **(U)** In most part-time manned/operated environments, locking the room door affords adequate protection.

23.3 (U) Part-time Manned - Full-time Operated. Part-time manned terminal spaces in which KG-84 or KIV-7 equipment is operated full-time must meet department/agency requirements for open storage of information classified at the level of the highest classified COMSEC key used in each such space.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

23.4 (U) Equipment Storage and Shipping. KG-84 and KIV-7 equipment and KYK-13, KYX-15, and AN/CYZ-10 fill devices must be zeroized prior to storage and shipping.

24. (U) Routine Destruction.

24.1 (U) Destroying Effective and Superseded Key. Except for daily cryptoperiod TEK that may be retained at user level outside its protective canister until each key setting is superseded and the last segment of redundant segment TEK intended for use with multi-station nets, KG-84 and KIV-7 key, in tape or electronic form, must be destroyed as soon as possible (but not longer than 12 hours) after it has been loaded into a KG-84 or KIV-7 equipment.

NOTE: (U) Since KG-84 and KIV OTAR TEK and OTAR KEK cannot be reused, its retention serves no purpose and can result in vulnerabilities.

24.1.1 (U) Daily Cryptoperiod TEK. KG-84 and KIV-7 TEK having daily cryptoperiods may be retained at the user level, in tape form or in fill devices, until the individual key setting is superseded.

24.1.2 (U) KIV-7 Remote Control Keys. KIV-7 RCTEK and RCKEK should be procured in a redundant segment format, such as the "ZC" format (2 copies each of 26 unique segments - monthly cryptoperiod) with biannual supersession. In COMSEC emergencies, single-copy punched tape key, such as the "IC" format (one copy each of 15 unique segments - monthly cryptoperiod) may be used as KIV-7 remote control TEK and KEK until authorized format key can be procured. Under this circumstance, users are authorized to retain effective segments until they are superseded.

24.2 (U) Disposing/Destroying Equipment. NSTISSI No. 4008 outlines procedures for reporting excess or unserviceable COMSEC equipment. When it has been determined that KG-84 or KIV-7 equipment is excess to U.S. Government needs, the heads or chiefs of the Federal departments, agencies, and Services may direct their respective subordinate elements either to demilitarize and dispose of it at the asset holding COMSEC account or to ship it to designated activities for demilitarizing and disposal, in accordance with NTISSI No. 4004.

NOTE: (U) Demilitarization involves removing classified and controlled cryptographic item components and transferring them to a facility that can securely destroy them. Unclassified equipment hulks may then be disposed of by any lawful means. In most situations, local disposal is the most cost-effective means for disposing of unwanted COMSEC equipment.

SECTION VIII - EMERGENCY PROCEDURES (U)

25. (U) Responsibility. In accordance with the provisions of NTISSI No. 4004, the safeguarding of KG-84 and KIV-7 equipment and related COMSEC material under emergency conditions is a responsibility of users and their commanders and supervisors. Reasonable efforts should be made to recover such materials lost through catastrophe or hostile action, but human life or personal injury should not be risked in recovery efforts.

SECTION IX - REPORTABLE COMSEC INCIDENTS (U)

26. (U) Sources of Guidance. Guidelines for reporting COMSEC incidents are stated in NSTISSI No. 4003. Specific reportable incidents affecting the KG-84 and KIV-7 systems are listed below:

26.1 (U) Updating. Updating a KG-84 or KIV-7 TEK, KEK, or start-up KEK more than 99 times.

26.2 (U) TEK Classification. Except in COMSEC emergencies, using a TEK having a lower classification than the highest classified information a KG-84 or KIV-7 net/circuit is authorized to transmit.

26.3 (U) KEK or Start-up Classification. Except in COMSEC emergencies, using a KEK or start-up KEK classified lower than the most highly classified TEK transmitted via OTAR or any key transmitted via OTAT.

26.4 (U) Cryptoperiod Extension. Unauthorized extension of a KG-84 or KIV-7 TEK, KEK, or start-up KEK cryptoperiod or of a KIV-7 RCKEK or RCTEK cryptoperiod.

26.5 (U) Key Abuse. Use of a KG-84 or KIV-7 key for an unauthorized purpose.

26.6 (U) Prohibited Modes of Operation. Except in COMSEC emergencies, using the KG-84 or KIV-7 automatic rekey/receive key (AK/RV) mode.

26.7 (U) Distributing KEK Electronically. Except in COMSEC emergencies, distributing KG-84 or KIV-7 KEK or start-up KEK via OTAR or OTAT.

26.8 (U) Retaining Effective or Superseded Key. Unauthorized retention of exposed segments of effective or superseded tape key or its electronic equivalent stored in a fill device.

26.9 (U) Use of KEK to Encrypt Traffic. Using OTAR KEK to encrypt traffic following a KG-84 or KIV-7 cold start.

26.10 (U) Unauthorized Use of Fill V. Using the "fill V" routine to key or rekey a KG-84 that terminates a net/circuit that is not rekeyed via OTAR, except where the terminal space is continuously manned by personnel who are cleared at least to the level of the TEK.

26.11 (U) Mishandling KIV-7 CIK. Finding a KIV-7 CIK installed or unsecured in the terminal space of the KIV-7 with which it is associated.

26.12 (U) Improper TEK Allocation. Use of the same TEK for more than one point-to-point circuit, i.e., to key collections of point-to-point circuits that do not qualify as nets.

ANNEX A

CLASSIFICATION, MARKING, AND ACCOUNTABILITY

Item	Classification/Marking	Accountability
KG-84A & KG-84C General Purpose Encryption Equipment	CCI	Serial #
KIV-7 & KIV-7(HS) Embeddable KG-84 COMSEC Module	CCI	Serial
AN/CYZ-10 (Unkeyed & Unlocked)	See Reference 1	Serial #
AN/CYZ-10 CIK	See Reference 1	Locally
KYX-15 (Unkeyed) Net Control Device	CCI	Serial #
KYX-15 (Keyed)	Highest Key Held	Quantity
KYK-13 (Unkeyed) Electronic Transfer Device	CCI	Quantity
KYK-13 (Keyed)	Highest Key Held	Quantity
KOI-18 General Purpose Tape Reader	CCI	Quantity
KAO-184 ( ) Guidelines for the Use and Operation of TSEC/KG-84 and TSEC/KG-84A	UNCLAS - FOUO	ALC-4
KAO-210 ( ) Guidelines for the Use and Operation of the KG-84C	UNCLAS - FOUO	ALC-4
Allied Signal 4065544-0201 KIV-7 Operation and Guidelines	UNCLAS - FOUO	None
KAM-411 ( ) Theory Textbook TSEC/KG-84A/KG-84	SECRET	ALC-1
KAM-412 ( ) Maintenance/Troubleshooting Manual KG-84A/KG-84	CONFIDENTIAL	ALC-1

Item	Classification/Marking	Accountability
KAM-330 ( ) Limited Maintenance Manual for Common Fill Devices KYK-13/TSEC, KYX-15/TSEC, and KOI-18/TSEC	CONFIDENTIAL	ALC-1
KAM-331 ( ) Maintenance Manual Common Fill Devices KYK-13/TSEC, KYX-15/TSEC, and JOI-18/TSEC	CONFIDENTIAL	ALC-1
LMM-2 ( ) Limited Maintenance Manual for KG-84C	UNCLAS - FOUO	Initial Receipt
LMM-5 ( ) Limited Maintenance Manual KG-84A/KG-84	UNCLAS - FOUO	Initial Receipt
LMM-8 ( ) Limited Maintenance Manual for AN/CYZ-10	UNCLAS - FOUO	Initial Receipt

* Accounting Legend Codes (ALCs) only apply to COMSEC material that is handled in the COMSEC Material Control System.

ANNEX B

REFERENCES

The following documents are referenced in this instruction:

1. DIRNSA memorandum, Serial: ISSO-086-93, Subject: Interim Operational Security Doctrine for the AN/CYZ-10 Data Transfer Device (DTD), 9 Jul 1993.

2. NACSI No. 4005, Safeguarding and Control of Communications Security Material,

   12 Oct 1979.

3. NACSI No. 4008, Safeguarding COMSEC Facilities, 4 Mar 1983.

4. NACSI No. 4009, Protected Distribution Systems, 30 Dec 1981.

5. NSTISSAM TEMPEST 2-95, Guidelines for Facility Design and RED/BLACK Installation, 1 Nov 95.

6. NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training, 1 Feb 1991.

7. NSTISSI No. 4001, Controlled Cryptographic Items, July 1996.

8. NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, 2 Dec 1991.

9. NSTISSI No. 4006, Controlling Authorities for COMSEC Material, 2 Dec 1991.

10. NSTISSI No. 4008, Program for the Management and Use of National Reserve Information Systems Security (INFOSEC) Material, 9 Aug 1991.

11. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, Jan 1996

12. NSTISSI No. 7000, TEMPEST Countermeasures for Facilities, 29 Nov 1993.

13. NTISSI No. 4002, Classification Guide for COMSEC Information, 5 Jun 1986.

14. NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, 11 Mar 1987.

15. NTISSI No. 4005, Control of TOP SECRET Keying Material, 17 Jul 1987.