NATIONAL SECURITY AGENCY

NAG-16F

(U) FIELD GENERATION AND OVER-THE-AIR DISTRIBUTION OF COMSEC KEY IN SUPPORT OF TACTICAL OPERATIONS AND EXERCISES

(U) HANDLING INSTRUCTIONS

1. (U) This document is effective upon receipt and supersedes NAG-16E, dated January 1999, which should be destroyed.

2. (U) Changes to this document will be promulgated by printed or message amendments that are to be entered upon receipt. Persons entering such amendments are expected to record entry on the Record of Amendments page.

3. (U) This document in not accountable in the COMSEC Material Control System. It may be reproduced without report, and extracts from it that are marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" may be made for official purposes.

4. (U) This document and its extracts may be used in aircraft.

5. (U) Foreign release of this document must be approved by the Director, National Security Agency.

MAY 2001

RECORD OF AMENDMENTS

AMEND NO.	DATE ENTERED	BY WHOM ENTERED

(U) FOREWORD

1. (U//FOUO) **Where Are We Heading**? - A major evolution in communications security (COMSEC) keying technology has begun. Under the Electronic Key Management System (EKMS) program, standards, hardware, and applications are being developed to apply state of the art automation to generate, distribute, load, control, and account for COMSEC key. The program incorporates sufficient backward compatibility to assure that both future, automated key and existing, common electronic key can be handled. EKMS hardware is being fielded, but full development of tailored tactical key generation and distribution programs may take several more years.

2. (U//FOUO) **Where Are We Now**? - Until EKMS Key Processors (KPs) and local management devices (LMDs) are fully implemented throughout the tactical forces, military commanders must be able to establish secure communications, without needless and/or redundant prepositioning of key or last minute key tape distribution. This document prescribes pre-EKMS techniques to satisfy that requirement, but emphasizes use of available EKMS terminals and other key variable generators (KVGs) to generate tactical key.

3. (U//FOUO) **Interoperability** - Effective and timely creation of secure tactical nets and circuits requires that communications planners and operators have a common base of understanding regarding applicable COMSEC procedures and equipment operating instructions. This document fulfills that requirement for Joint commands and their Service components. It also has limited applicability in multi-national operations and exercises, when the Allied participants use COMSEC equipment that is capable of over-the-air key distribution (OTAD).

NOTE: (U//FOUO) ACP-132A, **Field Generation and Over-the-Air Distribution of Key in Support of Tactical Operations and Exercises,** is the equivalent of NAG-16F for use by the military forces of Australia, Canada, New Zealand, and the United Kingdom. U.S. tactical forces do not hold ACP-132A, because its provisions are similar to those of NAG-16F.

NOTE: (U//FOUO) **N**AG-22A, **Over-the-Air Rekeying of Combined Tactical Nets and Circuits**, is a partial equivalent of NAG-16F intended to explain over-the-air rekeying (OTAR) to Allied users of “S” nomenclatured (special purpose) COMSEC equipment. When Combined nets/circuits include terminals equipped with “S” equipment, a U.S. station equipped with “K” nomenclatured equipment must serve as the net control station (NCS). U.S. tactical forces do not hold nor need NAG-22A.

NOTE: (U//FOUO) SDIP-14, **Operational Doctrine for TSEC/KW-46 Fleet Broadcast,** includes doctrine for Over-The-Air Transfer (OTAT) of tactical key via the single-channel North Atlantic Treaty Organization (NATO) fleet broadcasts. U.S. Navy (USN) tactical forces having NATO missions should hold SDIP-14.

4. **(**U//FOUO) **Implementation -** The principal advantage of the key management procedures presented here is flexibility to create a continuing supply of tactical key for a variety of commonly held COMSEC equipment and to distribute it electronically to potential users. The key generation and distribution routines given are particularly suitable for support of Joint operations and exercises involving forces that do not routinely train together. However, they cannot be relied upon to contribute to joint mission accomplishment, unless required levels of user competency are maintained through incorporation into intra-Service operations and exercises.

5. (U) **Assumption -** The keying routines presented herein assume that operators are familiar with the capabilities, operation, and safeguarding of the COMSEC equipment used and that secure communications capable of transmitting tactical key exist or can be established.

6. (U) **Relationship to National Directives** - NAG-16F incorporates innovative key distribution concepts that may not be reflected in national-level information systems security directives. Until the National Security Agency (NSA) can resolve and such conflicts, the provisions of NAG-16F constitute approved operational exceptions to the affected national directives.

7. (U) **Changes Reflected in NAG-16F** - The principal differences between NAG-16F and its predecessor, NAG-16E, involve:

a. (U) **KW-46** - A corrected OTAD routine for the KW-46 equipment used to secure U.S. Navy (USN) and U.S. Coast Guard (USCG) broadcasts, which was provided by Fleet Training Center Norfolk, VA, is reflected in Annex H.

b. (U//FOUO) **SINCGARS OTAD & ERF** - Because the user application software that has been developed for the data transfer device (DTD) has become so specialized, it is no longer feasible to publish a standard procedure for performing OTAD and electronic remote fill (ERF) for the various Single Channel Ground and Airborne Radio System (SINCGARS) securable radios. On the basis of an Army suggestion, the SINCGARS and ERF procedures that had been included as Annex F in NAG-16E have been omitted from NAG-16F. Users who find the previous SINCGARS OTAD and ERF procedures useful may clip them out of NAG-16E and retain them, before NAG-16E is destroyed.

c. (U) **Users of 128-bit TEK** - On the basis of another Army suggestion, the listing of contemporary U.S. COMSEC equipment that accepts 128-bit traffic encryption key (TEK), which had been included in NAG-16E as Annex K, has been omitted from NAG-16F. Here again, users who find that listing useful may clip it out from NAG-16E and retain it, before NAG-16E is destroyed.

d. (U) **OTAT via AUTODIN** - Because the Automatic Digital Information Network (AUTODIN) is being replaced by the Defense Message System (DMS), the paragraph in NAG-16E that had addressed the conduct of OTAT on AUTODIN has been omitted from NAG-16F.

e. (U//FOUO) **AN/CYZ-10** - Revised procedures for performing OTAD with AN/CYZ-10s, including provisions for transferring all types and classifications of COMSEC key between DTDs via Secure Telephone Unit (STU) - III, STU-IIIA, STU-IIB, and Secure Terminal Equipment (STE) secured telephone circuits, and OTAT of DTD transfer key encryption key (TrKEK) on EKMS-to-DTD circuits have been reflected in Annex I.

f. (U//FOUO) **ANDVT and KY-57/58/67 Cold Starting** - New **mandatory** cold starting procedures for KY-57/58/67 (See paragraphs 3.a. step 2 and 3.b. step 3 of Annex E.) and for KYV-5 and KY-99/99A/100 (See paragraphs 3.a. step 2 and 3.b. step 3.) of Annex F.)

g. (U//FOUO) **US-Only Key to Allies** - Authorization and criteria by which controlling authorities (CAs) of US-Only key may release it to Allies have been included in paragraph 3.h.(3)(a) on page 11 of the main section of NAG-16F.

h. (U//FOUO) **JTIDS Key and Data Transfers Via Secure Telephone Circuits** - Procedures for OTAT of Joint Tactical Information Distribution System (JTIDS) key and data between DTDs connected by secure telephone circuits that were developed by SPAWARSYSCEN San Diego are stated in Annex I.

8. (U) **Comments** - Holders of this document are encouraged to review it critically and to submit comments for its improvement, through command channels, to Director, National Security Agency, ATTN: I41T, Fort George G. Meade, MD 20755-6000.

9. (U//FOUO) **Action Officer** - The NSA NAG-16F action officer, Mr. Maguire, may be reached by phone at Defense Switched Network (DSN) 244-6804 or commercial (COML) (410) 854-6804.

MICHAEL J. JACOBS
Information Assurance
Director

THIS PAGE IS INTENTIONALLY BLANK

TABLE OF CONTENTS
(Also Serves as Index)

SUBJECT PAGE

SUBJECT PAGE

SUBJECT PAGE

SUBJECT PAGE

SUBJECT PAGE

(U) FIELD GENERATION AND OVER-THE-AIR DISTRIBUTION OF COMSEC KEY IN SUPPORT OF TACTICAL OPERATIONS AND EXERCISES

1. (U) INTRODUCTION

a. (U//FOUO) **Perspective -** Field generation and Over-The-Air-Distribution (OTAD) of the COMSEC key needed to support tactical communications offers distinct operational advantages over dependence on centrally produced, physically distributed tape key. Communications efficiency and flexibility can be materially enhanced, if secure tactical nets and circuits are established and rekeyed with field-generated TEK that is distributed via Over-The-Air Rekeying (OTAR). Pending full implementation of the Electronic Key Management System (EKMS), operational flexibility can also be enhanced if TEK for other tactical applications is distributed via Over-the-Air Transfer (OTAT), between Data Transfer Device (DTDs), using STU-III, STU-IIIA, STU-IIB, STE, or KY-68 secured telephone circuits, KW-46 secured broadcasts, or nets/circuits secured by KG-84A/C and KIV-7/7HS equipment. Commanders who generate and electronically distribute needed key have maximum latitude to structure their communications to support mission requirements and to react quickly to fluid tactical situations and potentially serious key compromises.

b. (U) **Purpose -** This document is intended as the standard U.S. user's manual for planning and conducting field key generation and OTAD in support of tactical activities. It is targeted primarily at Joint and Intra-Service Operations and Exercises, particularly those involving forces that do not routinely train or operate together. It also has limited application to Combined operations and exercises involving Allied forces that hold OTAR- and OTAT-capable COMSEC equipment.

c. (U) **Definitions & Acronyms -** Many of the specialized terms used in this document are defined in Annex A. Acronyms that appear in the document are also expanded in Annex A.

d. (U//FOUO) **Activation -** U.S. commanders at all echelons are authorized and encouraged to direct field generation and OTAD of keys needed to support tactical operations and exercises for which they are responsible.

> **NOTE:** (U//FOUO) The procedures addressed herein are presented as routine communications practices for tactical forces, but exceptions to certain specified COMSEC procedural constraints are authorized during COMSEC emergencies, in which the only viable alternative available to the responsible commander is plain text communications. The distinction between routine communications and COMSEC emergencies must be recognized, so that the emergency easements do not become standard operating practices, when the risks they entail should not be accepted. It is also important to note that the security easements permitted by this manual apply only in tactical applications and may not be extended to fixed-facility or strategic communications.

e. (U//FOUO) **Application to TRI-TAC & MSE -** The TRI-TAC and Mobile Subscriber Equipment (MSE) tactical communications systems have internal procedures for generating and distributing the keys they use; the provisions of this manual do not apply to those keys. However, due to the vital function they can perform in the production of keys intended for other applications, TRI-TAC/MSE KG-83 and KGX-93/93A KVGs and the KT-83 test equipment used to certify them

require special safeguards that do not apply to the other TRI-TAC/MSE COMSEC equipment. These are stated in the following subparagraphs.

(1) (U//FOUO**) Using KVGs & Fill Devices -** Any certified KVG having all of its tamper detection labels intact may generate 128-bit key at any classification level for any purpose, but fill devices into which KVGs load key must be safeguarded at the level of the most highly classified key they contain.

(2) (U//FOUO) **Certifying KT-83s & KVGs -** All KT-83s, KG-83s, and KGX-93/93As must be certified to the SECRET level at least every 24 months; none of these equipment need be certified to the TOP SECRET level. Each certification must be accomplished with a certified KT-83 and NSA-approved procedures and may be done by one qualified person who must be cleared at least SECRET. Any certified KT-83 with its tamper detection labels intact may be used to certify any other KT-83 or any KG-83 or KGX-93/93A. One result of this authorization is that any command that holds two or more KT-83s may stagger their certification dates and use one to certify the other, indefinitely. In COMSEC emergencies, responsible commanders are authorized to use KVGs with expired certifications, provided field certification is not feasible and certified replacements have been requisitioned.

(3) (U//FOUO) **Storing KT-83s & KVGs -** Tamper detection labels are required on all operational KVGs and KT-83s. After tamper detection labels have been applied to them, certified but uninstalled KG-83s, KGX-93/93As, and KT-83s may be stored and handled without Two-Person Integrity (TPI) controls. Installed KVGs may be stored in unmanned TRI-TAC and MSE shelters, if the following conditions are met:

(a) (U//FOUO) **Physical Safeguards -** Responsible commanders must ensure that adequate physical safeguards are provided for non-operational TRI-TAC/MSE shelters to minimize the risk of theft, tampering, or sabotage to all of the COMSEC equipment stored therein.

(b) (U//FOUO) **Tamper Detection Labels -** At the time of its last certification, NSA-furnished, coyote logo tamper detection labels must have been applied to each KT-83, KG-83, and KGX-93/93A, in accordance with NSA instructions. Certifying activities must record the serial numbers of the labels they apply to each KT-83 or KVG, so that this information may be made available to investigating elements, if tampering with a certified KVG is suspected. Recorded label serial numbers must also be compared with those removed from each KVG that is recertified at the same facility two or more consecutive times. Any unexplained serial number anomalies must be reported as COMSEC incidents.

NOTE: (U//FOUO) To increase the security of the coyote logo tamper detection labels, NSA has classified them SECRET prior to application; upon application, they are declassified. Any UNCLASSIFIED coyote logo labels on hand at using locations must be brought under SECRET protection. Pertinent questions may be referred to the NSA Protective Technologies Division at (301) 688-6816 of DSN 644-6816.

(c) (U//FOUO) **KVG Locking Bars -** Each KVG must be secured in its mounting by means of a hinged locking bar that is locked in place, on a TPI basis, by two combination locks.

(d) (U//FOUO) **KVG Inspections -** All KVG tamper detection labels must be visually inspected (by partially withdrawing the KVG from its mount) immediately before each KG-83 or KGX-93/93A activation. If the locking bar or any of the tamper detection labels is found to be damaged, the affected KVG loses its certification, and the circumstances must be reported as a COMSEC incident. However, use of a decertified KVG may begin or continue while the incident report is being evaluated.

f. (U//FOUO) **KY-68 OTAT -** OTAT procedures for TRI-TAC/MSE and sole-user (unswitched) KY-68 secured tactical voice circuits are stated in Annex G.

2. (U//FOUO) **OTAD-CAPABLE EQUIPMENT -** U.S. COMSEC equipment capable of generating key and/or of transmitting it via OTAD is identified in the following table:

EQUIPMENT	OTAR	OTAT	GENERATION
KY-57/58/67	X	X	X (1)
AN/CSZ-1A (2)	X		
KYV-5/KYX-99/99A/100	X	X	X (3)
KT-1523/1523A (4)	X	X	X (1)
AN/PRC-117C(C) (5)	X		
RT-1672C(C) (6)	X		
KG-84A/C	X	X (7)	
KIV-7/7HS (8)	X	X (7)	
AN/USC-61(C)(9)	X	X	
MIDS LVT(10)	X		
KW-46	X (11)	X	
KY-68		X	
DTD via STU-III/IIIA/IIB/STE (12)		X	
KGX-93/93A		X (13)	X
KG-83			X

1 - (U) Routine use authorized only for nets/circuits secured by KY-57/58/67, RT-1523/1523A, AN/PRC-117C(C) RT-1672C(C), AN/USC-61(C), and AN/CSZ-1A.

2 - (U//FOUO) SUNBURST processor. Compatible with KY-57/58/67, KYV-5 and KY-99/99A/100. May not serve as OTAR net control station (NCS). Capable of Automatic Rekeying (AK) OTAR, but not of Manual Rekeying (MK) OTAR or OTAT.

3 - (U) Routine use authorized only for nets/circuits secured by KYV-5/KY-99/99A/100, and AN/CSZ-1A.

4 - (U//FOUO) Single Channel, Ground/Air Radio System (SINCGARS) is compatible with KY-57/58/67. Provides Transmission Security (TRANSEC).

5 - (U//FOUO) SINCGARS. Compatible with KY-57/58/67. TRANSEC not compatible with RT-1523/1523A and not approved by NSA.

6 - (U) SHADOWFIRE interoperates with SINCGARS.

7 - (U) Outstations (OSs) extract key with KYX-15 or AN/CYZ-10.

8 - (U//FOUO) Modular equivalent of KG-84A/C. KIV-7HS is the high speed equivalent of the KIV-7.

9 - (U//FOUO) Navy Digital Modular Radio (DMR) is compatible with SINCGARS, KY-57/58/67, KG-84/KIV-7, KYV-5/KY-99/99A,100 (ANDVT), HAVE QUICK transceiver and AN/ARC-210 transceiver, and UHF SATCOM Demand Assigned Multiple Access terminal.

10 - (U//FOUO) Multifunctional Information Distribution System (MIDS) Low Volume Terminal (LVT) is capable of OTAR, but MIDS F-15 Fighter Data Link is not.

11 - (U//FOUO) KW-46 can OTAR only Community Variables (CVs).

12 - (U) Requires special connector cable (NSN 5810-01-391-4212) at sending and receiving terminals; see **NOTE** on page I-4 under paragraph 9.a. step 1.

13 - (U//FOUO) Capable of OTAT to other KGX-93s, using KG-82 and/or KG-112.

3. (U) **OTAD KEYING DOCTRINE**

a. (U//FOUO) **Key Requirements -** As a basis for employing the field key generation and OTAD schemes presented herein, commanders must identify lateral and subordinate commands that require common key for specific purposes and must direct generation and distribution of the needed key. Each commander who directs the generation of a COMSEC key becomes its Controlling Authority (CA).

b. (U) **Communications Paths -** When existing communications needed to accomplish OTAD are inadequate or unavailable, communications planners may be called upon to establish temporary nets or circuits to effect timely distribution of COMSEC key.

c. (U) **Types of Key**

(1) (U//FOUO) **TEK** is used to protect traffic passed on Point-To-Point (P-T-P) circuits and multi-station nets that are secured by KG-84A/C, KIV-7/7HS, KY-57/58/67, RT-1523/A, KYV-5/ KY-99/99/100 and KY-68 equipment.

NOTE: (U//FOUO) TEK used by STU-IIIs, STU-IIIAs, and STEs is cooperatively generated, on a per-call basis, by the conversing terminals.

NOTE: (U) When it is appropriate to make the distinction, TEK that is distributed via OTAR should be referred to as “OTAR TEK”, and TEK that is distributed physically, should be referred to as “non-OTAR TEK”.

NOTE: (U) Since EKMS terminals are not programmed to generate "KG-84 OTAR TEKs", operators must direct them to generate "KG-84 TEKs" for support of OTAD.

(2) (U//FOUO) **Key Encryption Key (KEK)** is used to protect TEK during OTAD on KG-84A/C, KIV-7/7HS, KY-57/58/67, RT-1523/A, KYV-5/KY-99/99A/100, and KY-68 secured nets and circuits and on KW-46 secured broadcasts. In tactical applications, KEKs (rather than start-up KEKs) should be used on communications nets and circuits that have stable compositions and that exist on a continuing basis.

(3) (U//FOUO**) Start-up KEK** is functionally similar to KEK, but is not dedicated to particular nets or circuits. Use of start-up KEK is appropriate when it is necessary to create temporary nets/circuits on short notice from, a predetermined group of tactical force terminals. With start-up KEK, any group of holders can create any number of nets or circuits secured by KY-57/58/67, KG-84A/C, KIV-7/7HS, KYV-5/KY-99/99A/100, RT-1523/A, and/or KY-68 equipment, with minimum pre-arrangement.

NOTE: (U) Using start-up KEK enhances flexibility and reduces the volume of tape key that must be held by tactical units.

(4) (U) **KW-46 Keys -** KW-46 secured broadcasts use the following keys:

(a) (U//FOUO) **Broadcast Area Variable (BAV) -** The USN uses separate BAVs for its broadcasts covering the Western Pacific/Indian Ocean area, the Eastern Pacific area, the Atlantic area, and the Mediterranean area. The USCG West Coast and East Coast/Gulf broadcasts use separate BAVs, and the NATO KW-46 secured broadcasts use separate BAVs for the Western Atlantic/Eastern Atlantic/Iberian area, the North Atlantic/Baltic Approaches area, and the Mediterranean/Black Sea area.

(b) (U//FOUO) **Community Variable (CV) -** A separate CV must be used for each channel of each USN surface ship and submarine general service (GENSER) fleet broadcast, for each USN special intelligence (SI) broadcast, for each USCG broadcast, and for each NATO broadcast. The same punched tape GENSER and SI CVs are used by Naval Computer and Telecommunications Area Master Stations (NCTAMSs) Pacific (Honolulu), Atlantic (Norfolk), and Central Europe (Naples). Under conditions when many carrier battle groups and amphibious ready groups are concentrated in a single fleet broadcast area, operational requirements for CVs may exceed the number of punched tape CVs available to a particular NCTAMS. When this occurs, the affected NCTAMS may generate additional CVs, using EKMS terminals or certified KVGs, and may allocate and distribute them electronically via OTAD.

NOTE: (U) EKMS terminals are not programmed to generate "KW-46 CVs", but can generate "KG-84 TEKs", which can serve effectively as KW-46 CVs.

(c) (U//FOUO) **TEK -** A "working" variable for each KW-46 secured broadcast channel and single-channel broadcast is formed by combining the appropriate BAV with the assigned CV.

(d) (U//FOUO) **KEK -** Cryptographically, KW-46 KEKs function like CVs. USN Pacific/Indian Ocean and USCG Pacific broadcasts use the same KEK for OTAT. USN Atlantic/

Mediterranean and USCG Atlantic/Gulf area broadcasts use another KEK in common, and all USN SI broadcasts use a single KEK. The NATO KW-46 broadcast OTAT KEK is AMST-4042.

(e) (U//FOUO) **Unique Variable (UV) -** Unique variables are used to decrypt KW-46 BAVs as they are loaded into each using equipment. A separate UV is assigned to each USN and USCG ship or activity that copies any USN KW-46 secured broadcast, and a separate NATO UV is assigned to each ship/station that copies any of the NATO broadcasts. Additionally, all USCG units that copy the Coast Guard East Coast/Gulf broadcast use a common UV, and all USCG units that copy the West Coast broadcast use a different, common UV.

(5) (U//FOUO) **Transmission Security Key (TSK)** is used to deny adversaries opportunities to exploit radio signals, thus protecting them from intercept and jamming. In the SINCGARS equipment, TSK is used to "wrap" other TRANSEC information (time of day, and either hopsets or frequency lockouts), by a process known as ERF, which may be used with radios not possessing COMSEC capabilities.

d. (U) **KEK Doctrine**

(1) (U) **KEK Generation & Distribution**

(a) (U//FOUO) **Routine Procedures -** Most KEK is NSA-produced and distributed physically, in punched tape form. Except in COMSEC emergencies, KEKs may not be distributed via OTAT over the nets/circuits on which they are used. However, when all users are located close enough to the producer so that distribution may be effected physically, KEK may be field-generated and delivered to users in keyed fill devices. Additionally, where it is necessary to do so, KEK may also be sent between DTDs that are connected by STU-III or STE secured secure voice circuits. EKMS terminals and certified KVGs may generate KEK for any of the OTAR-capable COMSEC equipment, but KY-57/58/67s and RT-1523/As may only generate KEK for use with those systems, and KYV-5/ KY-99/99A/100s may only generate KEK for use with those systems.

(b) (U) **Emergency Procedures -** In COMSEC emergencies, KY-57/58, KY-67, KYV-5, and KY-99/99A/100 equipment may generate KEK for use by any COMSEC equipment that requires it, and both centrally-produced and field-generated KEK may be distributed via OTAT on nets and circuits secured by any OTAT-capable COMSEC equipment.

(c) (U//FOUO) **TRI-TAC/MSE KEK Generation & Distribution -** Certified KVGs associated with TRI-TAC and MSE switches may generate KEKs classified SECRET and below for use in non-TRI-TAC/MSE applications. Such KEK may be routinely distributed via OTAT on TRI-TAC/MSE circuits, but key identification or "tagging" information must be passed separately on secure TRI-TAC/MSE orderwires.

NOTE:(U//FOUO) NCSs using this method should distribute the next-up KEK one cryptoperiod in advance, so it will be available to support unscheduled cold starts on the using nets or circuits.

(2) (U//FOUO) **Cold Start -** A cold start is required each time a KG-84A/C, KIV-7/7HS, KY-57/58/67, KYV-5/KY-99/99A/100, RT-1523/A, or sole-user KY-68 secured net or circuit that rekeys via OTAR is initially activated and when a keyed COMSEC equipment fails or must be

replaced for any other reason at either terminal of a P-T-P circuit. If fresh fill hold batteries are used to hold key in COMSEC equipment, cold starts should not be required because of power failures or circuit path interruptions, or when OTAR is initiated on an operational net/circuit. Cold start routines for KG-84A/C and KIV-7/7HS, KY-57/58/67, KYV-5, KY-99/99A/100, and KY-68 equipment are shown in Annexes D thru G, respectively.

NOTE: (U//FOUO) There is no relationship between the replacement of KEK and TEK. When it is necessary to replace the KEK on a net or circuit that distributes TEK via OTAR, it is not necessary to zeroize the TEK in use and to perform a cold start. Shortly before the time scheduled for each KEK replacement, the NCS should remind the OSs that a KEK replacement is about to occur. The NCS should also direct the OS(s) not to zeroize their effective TEK.

(3) (U//FOUO) **KEK Classification -** Each KEK is classified at the level of the highest classified TEK it secures. In COMSEC emergencies, any uncompromised classified, 128-bit key that is held in common by the affected commands and that is not used for any other purpose, may serve temporarily as KG-84A/C, KIV-7/7HS, KY-57/58/67, KYV-5/KY-99/99A/100 or KY-68 KEK, until properly classified KEK can be provided.

(4) (U) **KEK Allocation**

(a) (U//FOUO) **Multi-Station Nets -** OTAR on KY-57/58/67, KYV-5/KY-99/99A/100, KG-84A/C, and KIV-7/7HS secured multi-station nets may be accomplished either sequentially, one OS at a time, or simultaneously for all net OSs. The simultaneous approach is attractive in large or slow-speed nets, where the time required to complete a sequential OTAR cycle would be operationally unacceptable. However, the sequential approach is less prone to operator error. If a NCS selects the sequential method, multiple KEKs are used, and each OS or group of OSs is assigned a unique KEK. When the simultaneous approach is used, all net OSs must hold common KEK (or start-up KEK). When it is operationally advantageous to do so, as might be the case when some OSs are particularly vulnerable to capture, the two schemes may be combined. The NCS may then allocate KEK so that each vulnerable OS holds a unique KEK, while the other OSs hold a common KEK. The NCS of each tactical net that rekeys with OTAR should consider carefully the method by which net KEK will be allocated.

NOTE: (U//FOUO) Creation of a net with start-up KEK automatically provides common KEK for all net OSs and mandates simultaneous OTAR.

(b) **P-T-P Circuits -** Each KG-84A/C, KIV-7/7HS, KY-57/58/67, KY-68, or KYV-5/KY-99/99A/100 secured P-T-P circuit that distributes TEK or TSK via OTAD must use a unique KEK. In COMSEC emergencies, common KEK may be used for all P-T-P circuits controlled by a NCS, until separate, two-copy KEK can be provided for use with each OS.

(5) (U//FOUO) **KEK Cryptonet Size -** The number of holders of each centrally-produced and field-generated KEK should be kept as small as possible. Where tape KEKs are used, CAs may order a reasonable number of extra copies to accommodate future net expansion, but NSA may challenge tape copy counts of over 50.

NOTE: (U//FOUO) Some COMSEC account other than the U.S. National Distribution Authority (NDA) holds uncommitted, extra copies of distributed KEK or other types of key. Normally the CA's account performs this function.

(6) U//FOUO) **KEK Cryptoperiods -** The maximum cryptoperiod for each OTAD KEK is three months. CAs may extend KEK cryptoperiods for up to 7 additional days without report, but longer extensions must have prior NSA approval or be reported as COMSEC incidents.

NOTE: (U//FOUO) The cryptoperiod for each segment of KEK is unaffected by the subsequent supersession of the canister from which it was drawn. *Example*: If a segment of KEK tap becomes effective on 1 February and the canister from which it was taken supersedes on 1 April, the KEK segment cryptoperiod runs through 30 April.

(7) (U) **KEK Supersession**

(a) (U//FOUO) **Tape KEK -** Each edition of tape KEK that supports a continuing net/ circuit is superseded annually; resupply is automatic, without further action by the CA. Tape KEK intended for use with nets and circuits that operate intermittently may be requisitioned on an irregularly superseded basis. However, irregular supersession places the burden of ensuring continuing re-supply on the CA, who should allow at least four months for central production and physical distribution of requisitioned follow-on editions.

(b) (U//FOUO) **Field-generated KEK** is superseded at three month intervals or at the conclusion of the tactical operation or exercise in which it is used, whichever is shorter.

e. (U) **Start-up KEK Doctrine -** Start-up KEK is the basis for activating tactical nets and circuits that distribute TEK via OTAR, but that do not have a designated KEK. Except as amended or amplified below, the procedures expressed in paragraph 3.d. apply to start-up KEK

(1) (U//FOUO) **Start-up KEK Production & Distribution -** U.S. military commanders at all echelons may requisition start-up KEK. Such key must be prepositioned in tape form or converted from tape to electronic form and delivered physically in fill devices. In COMSEC emergencies, individual segments of start-up KEK may be distributed via OTAT.

(2) (U//FOUO) **Start-up KEK CA Responsibilities -** The CA for each start-up KEK must designate and maintain accurate records of its holders, must designate its potential NCSs, and must ensure that each potential NCS holds a KYX-15 (or a DTD) and a source of TEK (either a single copy tape TEK or access to an EKMS terminal or a certified KVG).

(3) U//FOUO) **Start-up KEK Holders & Cryptonet Size -** Holders of each start-up KEK must be U.S. or Allied military commands that have potential need to participate in KY-57/58/67, KYV-5/KY-99/99A/100, KG-84A/C, or KIV-7/7HS secured nets and circuits, that is, they must constitute a pre-determined community of interest. Cryptonet sizes should be kept as small as possible, and NSA may challenge requests for production of start-up KEKs having copy counts higher than 250.

(4) (U//FOUO) **Start-up KEK Segment Count, Cryptoperiod and Supersession -** Each edition of start-up KEK is produced in the "VA" format (62 segments - daily cryptoperiod) and is

effective for two months. Segment use is based on a predictable day/date relationship. Segments 1A thru 31A are available for establishing nets and circuits during the first month an edition is effective, and segments 1B thru 31B are available for establishing nets and circuits during the second month. For example, segment 5B may be used only on the fifth day of the second month an edition is effective.

(5) (U//FOUO) **Start-up KEK Use -** Where all stations that need to communicate hold more than one start-up KEK of the required classification, the NCS should use the start-up KEK having the smallest number of holders. On its effective date, a segment of start-up KEK may be used by any of its designated NCSs to activate any number of KY-57/58/67, KYV-5, KY-99/99A/100, KG-84A/C, or KIV-7/7HS secured nets or circuits, without specific authorization from the CA. The NCS must notify the prospective OSs via secure communications of the date and time the net/circuit will begin operation, the short title and segment of start-up KEK to be used, the COMSEC equipment affected, and communications path involved. In COMSEC emergencies, unsecured communications may be used for such notification. Segments of start-up KEK must not be extracted from their protective canisters until shortly before they are required to create authorized tactical nets or circuits. At that time, lower-numbered tape segments and their electronic equivalents must be destroyed within 12 hours.

(6) (U//FOUO) **ICP Start-up KEK Use -** The Joint Intertheater COMSEC Package (ICP) includes SECRET USKAT B13333 and TOP SECRET USKAT B13334 start-up KEKs. These keys may be used to establish tactical nets/circuits that will distribute TEK via OTAR, only when no other start-up KEK (or KEK) is held in common by prospective net/circuit members.

f. (U) **TEK Doctrine**

(1) (U//FOUO) **Sources of TEK -** To the maximum feasible extent, commanders should field-generate the TEK needed to support their operations and exercises. Field generation of TEK is accomplished by EKMS terminals, by certified KG-83s/KGX-93s, by KY-57/58/67s, or by KYV-5/ KY-99/99A/100s. One-copy, centrally-produced tape key may also be used as TEK. In COMSEC emergencies, any uncompromised, tape key that is controlled by the using NCS and that is not used for any other purpose may be used as TEK.

(a) (U//FOUO) **TEK Generation with Certified KVGs -** TEK intended for use with any COMSEC equipment that uses 128-bit key may be generated by certified KG-83/KGX-93s. KG-83s and KGX-93s must be certified before initial use and recertified every two years. In COMSEC emergencies, KG-83s/KGX-93s with expired certifications may be used, pending recertification or replacement with a certified equipment.

NOTE: ((U//FOUO) KVGs certified to SECRET level may be used to generate key at any classification and for any purpose, provided prescribed security procedures are applied to keyed fill devices into which such key is loaded. When TOP SECRET or sensitive compartmented information (SCI) key is generated and stored in an HGX-83 or KGX-93/93A, all personnel allowed access to the stored key must be appropriately cleared. Where NSA waivers are in place to accommodate certain exceptions to this procedure, compliance with the requirements of those waivers is mandatory.

(b) (U) **Key Generation with LMD/KP** - EKMS Local LMD and KP equipped terminals are being introduced throughout the Department of Defense. Like certified KVGs, LMD/KPs are capable of generating unlimited quantities of 128-bit key, but the LMD/KP offers an important operational advantage over KG-83 and KGX-93/93A key generation, in that it is capable of loading up to 1,000 OTAR TEKs into a DTD using one series of commands, rather than one key at a time. Users of OTAR TEK are encouraged to use LMD/KP key generation whenever possible.

NOTE: (U//FOUO) Simple sequential numbering (e.g., 1 - 1,000) may be used to tag OTAR TEKs generated by an LMD/KP. No record keeping, other than that which takes place automatically through the LMD/KP and DTD audit trails, is required for such keys.

(c) (U) **TEK Generation with KY-57/58/67 and KYV-5/KY-99/99A/100 -** KY-57/58/67s and KYV-5/KY-99/99A/100s are only authorized to generate TEK for use by their respective COMSEC equipment families. In COMSEC emergencies, KY-57/58/67 and KYV-5/KY-99/99A/100 equipment may be used to generate TEK for any COMSEC equipment used to support tactical operations.

(2) (U) **TEK Distribution**

(a) (U//FOUO) **Methods -** To the maximum feasible extent, commanders should distribute TEK via OTAD, e.g., each carrier battle group should generate and distribute intra-battle group TEK, rather than requesting that it be sent on a fleet broadcast. TEK may also be distributed physically, in tape form or in loaded fill devices.

(b) (U) **TEK Implementation**

"1" (U//FOUO) **GENSER TEK -** If OTAT is accomplished on a net/circuit that uses KEK of the proper classification, any TEK intended for tactical, GENSER use may be distributed via OTAT.

"2" (U//FOUO) **SCI/SI TEK -** TEK intended for use on tactical, SCI or SI nets, circuits, or broadcasts may only be distributed on SCI/SI nets/circuits or broadcasts that use KEK of the proper classification.

(3) (U//FOUO) **TEK Classification -** TEK is classified at the level of the most highly classified information normally transmitted on the net, circuit, or broadcast with which it is associated. Although field-generated TEK cannot be marked with a classification, fill devices must be protected at the level of the most highly classified key or information they contain that can be accessed.

(4) (U//FOUO) **TEK Allocation -** A unique segment of TEK tape or a unique field-generated TEK must be used on each tactical net or circuit.

(5) (U) **TEK Cryptoperiods**

(a) (U) **Cryptoperiod Norms**

"1" (U) **Tactical Secure Voice TEK -** One month is the normal cryptoperiod for full-time, tactical KY-57/58/67 and KYV-5/KY-99/99A/100 TEKs.

"2" (U//FOUO) **Data TEK -** Either one week (for OTAR applications) or one month with daily update (for non-OTAR applications) are the normal crypto- periods for full-time, tactical KG-84A/C and KIV-7/7HS TEKs.

"3" (U//FOUO) **TEK Cryptoperiod Extensions -** Using commanders may authorize temporary, local extensions of voice and data circuit/net TEK cryptoperiods to complete ongoing operational activity, such as recovering tactical aircraft that are airborne at key change time. Tactical commanders who authorize such extensions assume the responsibility to notify other commanders whose forces may be affected. Notification of the CA is required only for extensions that are longer than one day.

(b) (U//FOUO) **Special Situations -** NCSs may specify mission length TEK cryptoperiods up to one month, that do not coincide with calendar months, for nets/circuits secured by KY-57/58/67, KYV-5/KY-99/99A/100, KG-84A/C, and KIV-7/7HS crypto- equipment. Also, where highly sensitive traffic is being transmitted, NCSs may specify TEK periods that are shorter than the stated tactical norms.

g. (U//FOUO) **KW-46 OTAD -** KW-46 secured broadcasts are particularly well suited to distributing COMSEC key to widely dispersed surface forces afloat. In addition to transferring U.S. Navy, Coast Guard, and Marine Corps-controlled key to forces afloat, U.S. broadcasts may be used to transfer Allied key, joint key, and key controlled by U.S. Army and U.S. Air Force commanders. NATO has adopted OTAT as a means of distributing key to its forces afloat using KW-46 secured, NATO broadcasts. U.S. and NATO KW-46 secured broadcasts may also be used to transmit KW-46 CVs via OTAR or OTAT. Guidance for implementing broadcast OTAD is expressed below:

(1) (U//FOUO) **Limiting Distribution -** In U.S. multi-channel, KW-46 secured broadcasts, OTAD must be conducted on channels that serve the intended recipients but that have the narrowest distribution. For example, key intended for a carrier battle group should be sent on a dedicated channel, rather than the "common" channel.

(2) (U//FOUO) **OTAT on GENSER Broadcasts -** USN and USCG GENSER broadcasts may transfer, via OTAT, GENSER TEK that is classified up to the level of the BAV/CV used on the transmitting broadcast or broadcast channel.

(3) (U//FOUO) **OTAT on SI Broadcasts -** U.S. Navy SI broadcasts may transfer any key intended for tactical use. However, SCI and SI key may only be transferred via OTAT on SI broadcasts, nets, and circuits.

(4) (U//FOUO) **CV OTAT/OTAR -** KW-46 CVs that are field-generated or converted from tape may be distributed on KW-46 secured broadcasts via OTAT, for extraction into a fill device, or via OTAR, for use in the receiving KWR-46.

(5) (U//FOUO) **KEK OTAT/OTAR -** KW-46 KEKs and other KEKs and start-up KEKs must be distributed physically, normally in tape form. In COMSEC emergencies, keys of these types may be distributed via OTAT on KW-46 secured broadcasts.

h. (U) **OTAR on Combined Nets & Circuits**

(1) (U//FOUO) **Background -** Some Allied nations intercommunicate securely with U.S. forces using standard ("K" nomenclatured) COMSEC equipment they purchase from the United States or produce. with U.S. authorization. Others inter-communicate using special-purpose ("S" nomenclatured) equipment they lease from the United States, and still others intercommunicate using cryptographically compatible, national COMSEC equipment that may or may not be capable of OTAR. Some Allied nations have adopted OTAR as a routine means for rekeying tactical nets and circuits, but others have not done so and do not hold DTDs or KYX-15 fill devices needed to perform NCS functions. For these reasons, OTAR during Combined operations and exercises must be planned and implemented on a case-by-case basis.

(2) (U//FOUO) **Feasibility -** Allied OSs in Combined nets and circuits secured by KG-84A/C or KIV-7/7HS and/or SG-84A/C, KY-57/58 and/or SY-57/58, and KYV-5/KY-99/99A/100 and/or SYV-5/99 equipment may be rekeyed via OTAR, if they hold properly configured KEK in common with a U.S. NCS. OTAR may not be technically feasible on Combined nets/circuits secured by other types of COMSEC equipment.

(3) (U) **Keying**

(a) (U//FOUO) **"K" Equipment Key -** KEK and TEK used on Combined nets and circuits that involve only "K" nomenclatured COMSEC equipment are normally nomenclatured "AKAT". When operationally necessary, CAs are authorized to release US-Only keys they control to specified Allied users for specified periods. When this is done, all U.S. holders must be notified and no releases of U.S. COMSEC equipment may be involved.

(b) (U//FOUO) **"S" Equipment KEK -** On Combined nets or circuits that include any "S" nomenclatured equipment, the KEK used by OSs having such equipment is nomenclatured "ASAT". KEK used by the NCS and all U.S. or Allied OSs using "K" nomenclatured equipment bears the same number, but is nomenclatured "AKAT", for example, ASAT-1234/AKAT-1234.

(c) (U//FOUO) **"S" Equipment TEK -** On Combined nets or circuits that include any "S" nomenclatured equipment, U.S. produced tape TEK nomenclatured "AKAT", as well as field-generated TEK may be transmitted to U.S. and Allied OSs via OTAR. In COMSEC emergencies, tape TEK nomenclatured "USKAT" may also be transmitted, on a case-by-case basis, with permission of the CA.

(d) (U) **Release of Start-up KEK -** Foreign release or OTAD of start-up KEK nomenclatured "USKAT" must be specifically authorized by the CA. Start-up KEK nomenclatured "AKAT" may be furnished to authorized Allied holders.

4. (U) **OTAD IMPLEMENTATION**

a. (U) **Identifying Electronic Key -** Field-generated TEK that is distributed via OTAR is not labeled, since it is delivered directly into NCS and OS COMSEC equipment. However, identification must be assigned to each key that is distributed via OTAT to support written record keeping at the

stations that send, receive, and relay such key. Of the COMSEC equipment capable of OTAT, only the DTD can transmit the electronic identification or "key tag" associated with each key it transfers. For this reason, identification must be included in all DTD key transfers. When key is transferred via OTAT on a KW-46 secured broadcast or a net or circuit secured by KY-57/58/67, KYV-5/KY-99/99A/100, KG-84A/C, KIV-7/7HS, or KY-68, equipment, key identification must be sent by separate transmissions. Annex C presents sample log formats for OTAT activity.

(1) (U//FOUO) **Identifying Field-generated Key -** The commander who orders field generation of a key must ensure that it is assigned an appropriate identification. One identification scheme is "##LLLLL###", where "##" is the sequential number among keys generated on a particular day, "LLLLL" identifies the controlling authority, and "###" is the Julian date of generation. "0852ID180" would identify the eighth key generated for the 52nd Infantry Division on the 180th day of the calendar year. Key tags should not exceed ten characters, and the "LLLLL" portion may include letters and numerals, and may have fewer than five characters.

(2) U//FOUO) **Identifying Converted Key -** Identification of electronic key that originated as key tape is derived from the short title, edition, and segment number of the tape used. A recommended approach is "L#####LL##", where "L" shows either "U" for U.S-only key or "A" for allied key, "#####" shows the four or five digits of the short title, "LL" represents the one or two letters of the edition number, and "##" is the one or two digits identifying the tape segment number. "U634D05" would be the identification of the fifth segment of USKAT-634D.

b. (U//FOUO) **OTAD with ICP Key -** OTAD using ICP keys is limited to holders and users who have been validated by the Joint COMSEC Manager, a Unified Commander-in-chief (USCINC), or, if the USCINC so requests, a Joint Task Force Commander. Exceptions may be requested via message addressed for action to the theater headquarters, and for information to the Joint COMSEC Manager and appropriate Service Component Commanders. Emergency exceptions may be requested via secure telephone from the Joint COMSEC Manager (DSN/STU-III 968-2461) or via facsimile at DSN/STU-III 968-6502.

(1) (U//FOUO) **Using ICP Start-up KEK -** The Joint ICP includes SECRET USKAT B133333 and TOP SECRET B13334 start-up KEKs. When no other KEK or start-up KEK is held in common by U.S. commands that must transfer key via OTAD on nets/circuits secured by KG-84A/Cs, KIV-7/7HS, KY-57/58/67s, KYV-5, KY-99/99A/100s, or KY-68s, the responsible commander may direct use of the appropriate ICP start-up KEK to establish such nets and circuits. Specific authorization to do so need not be requested from the Joint COMSEC Manager, and no report of use need be made.

(2) (U//FOUO) **Using ICP Generic Key** - The Joint ICP also includes a generic key, USKAT-5360, that is assigned on a segment-by-segment basis to fulfill unplanned 128-bit key requirements. When a designated segment of USKAT-5360 is assigned for use by a particular set of holders, it normally becomes necessary for them to extract unwanted, lower-numbered segments from the effective canister. To ensure that these by-passed segments are securely stored and available if the holding unit is directed to join nets that use them, they must be sealed in opaque, tamper-evident, plastic bags; see paragraph 4.l.(4) on page 12.

(a) (U//FOUO) **Using ICP Generic Key as KEK -** When neither USKAT-B13333/B13334 nor any other KEK or start-up KEK is held in common by commands that must

communicate via nets/circuits secured by KG-84A/C, KIV-7/7HS, KY-57/58/67, or KYV-5/KY-99/99A/100 equipment, the responsible commander may request that the Joint COMSEC Manager authorize use of a designated segment of USKAT-5360, the ICP generic key, as the start-up KEK on such nets/circuits. Address message requests to do this for action to the JOINT COMSEC MANAGER MACDILL AFB FL and information to affected USCINCs. Use of USKAT-5360 may also be requested by secure telephone or facsimile.

(b) (U//FOUO) **Using ICP Generic Key as TEK -** When a NCS that must establish a net/circuit secured by KG-84A/C, KIV-7/7HS, KY-57/58/67, KYV-5, KY-99/99A/100, or KY-68 equipment has no other source of TEK, the responsible commander may request that the Joint COMSEC Manager authorize use of designated segments of USKAT-5360 for that purpose.

c. (U//FOUO) **Key Transfer Between DTDs via STU-III/STU-IIIA/STU-IIB/STE -** Key of any classification for any purpose may be transferred between DTDs via STU-III, STU-IIIA, STU-IIB, or STE secure voice circuits, provided the affected terminals are authorized to handle information classified at the level of the transmitted key. In COMSEC emergencies, key that is classified higher than that level may be transferred.

CAUTION: (U) DTDs must be connected to STU-III/STU-IIIA/STU-IIB/STEs by a special connector cable (NSN 5810-01-391-4212) that is not furnished with the DTD, but that may be ordered from USACSLA Ft. Huachuca, AZ (Code SELCL-IA) at a cost of about $35 each.

d. (U//FOUO) **Key Transfer Between EKMS Terminals & DTDs** - Key of any classification for any purpose may be transferred from EKMS terminals to local or distant DTDs, provided the TrKEKs used are classified at least at the level of the transferred key. In COMSEC emergencies, key that is classified higher than the level of the TrKEK being used may be transferred.

NOTE: (U//FOUO) Provided the protocol “E-FILL 410" has been implemented on the affected EKMS terminal, and a distant using activity has at least two DTDs that hold different TrKEKs, new TrKEK for one DTD may be transferred via OTAT to the other DTD and vice versa. This practice may continue indefinitely and obviates the inconvenience and physical risks associated with returning DTDs to their host EKMS terminal for replacement of TrKEK.

e. (U) **Key Transfer via TRI-TAC and MSE**

(1) (U//FOUO) **Inter-switch Key Transfer -** Key intended for use outside TRI-TAC and MSE applications may be transferred between MSE node center switches and large extension nodes, between AN/TTC-42 switches (using “command 11" procedures), and between TRI-TAC AN/TTC-39D switches. However, AN/TTC-39A switches do not have that capability. When key is transferred between MSE and AN/TTC-39D switches and extracted into KYK-13s or KYX-15s, associated key identification must be transmitted separately. Key generated by AN/TTC-39A switches can only be extracted into fill devices at the generating sites.

(2) (U//FOUO) **Key Transfer via KY-68 -** When under control of a KYX-15 or DTD, the KY-68 can perform OTAT, using manual cooperative variable transfer procedures, as stated in Annex G.

NOTE: (U//FOUO) When the DTD is used, the KY-68 also transfers the tags associated with the transferred keys. However, key tags must be passed separately, by use of the orderwire or some other means, when the KYX-15 is used to input or extract the transferred key.

f. (U) **Problems & Special Situations -** NCSs responsible for conducting OTAD on KG-84A/C, KIV-7/7HS, KY-57/58/67, KYV-5/KY-99/99A/100 or KY-68 secured nets and circuits must plan ahead to deal with unforeseen problems, such as equipment or communications path failures and operator mistakes, as well as predictable problems, such as late joiners.

(1) (U) **Unsuccessful OTAR -** NCS and OS COMSEC equipment operators must know, in advance, the fallback arrangements to be used if an unsuccessful OTAR disrupts secure communications.

(a) (U//FOUO) **Plain Text Override Fall-back -** One means of accommodating the fall-back requirement for KY-57/58/67 and KYV-5/KY-99/99A/100 secured nets and circuits is to take advantage of the plain text override capability of these equipment. In COMSEC emergencies, OSs experiencing OTAD difficulties may call their NCSs in-the-clear and advise of their specific problems. Another technique involves the NCS keeping a separate KY-57/58/67 or KYV-5/KY-99 keyed with the net or circuit KEK in a TEK fill position, so that an OS experiencing difficulty may securely communicate with the NCS to explain the problem.

(b) (U//FOUO) **Secure Voice Fall-back -** When STU-III, STU-IIIA, STU-IIB, or STE terminals and interconnecting communications are available to the NCS and an OS of a KY-57/58/67, KYV-5/KY-99/99A/100, KG-84A/C, KIV-7/7HS, or KY-68 secured net/circuit, they may be used to report and recover from OTAD problems. DTDs connected to STU-III/STE terminals may also be used to transfer key to afloat commands that missed its transmission on a secure broadcast.

(2) U//FOUO) **Late Joiners & Rejoiners -** When an authorized OS is unable to join a KG-84A/C, KIV-7/7HS, KY-57/57/67, or KYV-5/ KY-99/99A/100 secured net on the day it was established or must leave and rejoin such a net after one or more key changes have taken place, the NCS must provide it with the effective TEK via secure means.

(a) (U//FOUO) **OS Holds Net Start-up KEK -** If the late joiner or rejoiner holds the net start-up KEK the NCS can provide it with the effective TEK, via OTAR, using the start-up KEK that is effective for the date on which the late joiner or rejoiner enters the net.

(b) (U//FOUO) **OS Holds Net KEK -** If the late joiner or rejoiner holds the net KEK but is unaware of the current KEK update count, the NCS must advise the OS, by secure means, of the KEK update in effect. In COMSEC emergencies, that information may be transmitted via unsecured means. The NCS can also cold start the net, with the additional OS included.

NOTE: (U) To prepare for possible late joiners and rejoiners entering a net, the NCS operator must keep accurate records of the number of times the KEK of his COMSEC equipment has been updated.

(c) (U//FOUO) **NCS & OS Hold Other Key in Common -** If a NCS can confirm that it holds any uncompromised, U.S. classified key in common with a late joiner or rejoiner, it may use such key to OTAT needed TEK to the OS.

g. (U//FOUO) **Establishing Additional Nets/Circuits -** Once an OTAD-capable KG-84A/C & KIV-7/7HS or KYV-5/KY-99/99A/100 secured net or circuit is established with a late joiner or rejoiner, the NCS can transfer TEK and TSK for other nets and circuits to the joining OS via OTAT. In COMSEC emergencies, KY-57/58/67 secured nets or circuits may also be used for that purpose.

h. (U) **Alerting Receivers -** Before distributing key via OTAT or MK OTAR, the sender should advise intended recipients of his intentions.

i. (U) **Record Keeping -** Stations that transmit, relay, or receive key via OTAT must maintain local records, to verify that intended delivery has been accomplished. Local records should be retained at least for the duration of the effective cryptoperiod of the key. Suggested log formats are presented in Annex C.

j. (U//FOUO) **Reporting and Evaluating COMSEC Incidents -** It is essential that each incident that jeopardizes key be reported expeditiously, in accordance with applicable Service instructions. In most cases, such reports are sent by messages addressed for action to the CA, who then becomes responsible for evaluating the reported incident and for directing measures to minimize its security impact. For field generated key, priority should be given to directing replacement of jeopardized key.

k. (U//FOUO) **Operating Procedures -** Concise operating procedures for cold starting nets and circuits secured by KG-84A/C, KIV-7/7HS, KY-57/58/67, KYV-5, KY-99/99A/100, and KY-68 equipment, for keying such nets and circuits, and for conducting OTAR and OTAT on them are stated in Annexes D - G. Operating procedures for performing OTAT (and CV OTAR) on KW-46 secured broadcasts are expressed in Annex H, and operating procedures for using DTDs to emulate KYX-15 and KYK-13 common fill devices and for transferring key and data tags between DTDs over P-T-P circuits that are secured by STU-III/STU-IIIA, STU-IIB, and STE are stated in Annex I.

l. (U//FOUO) **Safeguarding Exposed Key** - COMSEC key tape segments that have been removed from their protective canisters for use or for any other authorized purpose are highly vulnerable to human intelligence exploitation, e.g., copying for sale to a hostile interest. Several means for reducing that vulnerability are discussed below.

(1) (U//FOUO) **Redundant Segment Key Tape Formats** - CAs should deter- mine whether the holders of each of the TEKs they control are normally expected to enter, leave, and reenter the using net during individual cryptoperiods, e.g., where a Coast Guard aircraft or small surface craft joins and leaves a drug interdiction net several times in the same month. Where this is the case, the CA should request a format change that provides an appropriate number of redundant copies of each unique key tape segment. Use of the redundant segment approach allows holders to

destroy most segments shortly after they are loaded for use and obviates most segment retention. Redundant Segment key tape formats available to CAs are listed in the following table:

Production Digraph First Letter	Unique Key Segments	Copies Per Segment	Total Segments Per Edition
B	5	3	15
C	1	5	5
D	6	5	30
F	1	10	10
H	1	31	15
K	6	12	72
R	4	5	20
W	1	65	65
Y	26	2	52
Z	15	5	75

NOTE: (U//FOUO) To ensure that effective key will always be available for use, the final segment of a redundant segment TEK (and/or its electronic equivalent stored in a fill device) may be retained, in secure storage, through-out the remainder of its cryptoperiod. This easement does not apply to single-copy format keys, such as “V format” (1 copy each of 62 unique segments) TEKs and “G format” (1 copy each of 16 unique segments) KEKs. With some important exceptions noted below, effective segments of single-copy keys must be securely destroyed within 12 hours after they are loaded for use.

(2) (U//FOUO) **Start-Up KEK** - The Joint ICP includes SECRET USKAT B13333 and TOP SECRET B13334 start-up KEKs. Segments of these and all other start-up KEKs must not be extracted from their protective canisters until shortly before they are required to create authorized tactical nets or circuits. At that time, lower-numbered tape segments must be destroyed within 12 hours. Since each segment of start-up KEK may be implemented at any time during its effective day, it and/or its electronic equivalent should be retained, in secure storage, throughout the remainder of its one-day cryptoperiod. Following supersession, start-up KEKs in tape form or its electronic equivalent stored in a fill device must be securely destroyed within 12 hours.

NOTE: (U//FOUO) Effective segments of start-up KEKs may be stored in tamper-evident plastic bags, but this is not mandatory.

(3) (U//FOUO) **TRI-TAC Switch Interconnect Keys** - Another major grouping of ICP keys (USKAT 60501 - 60580) are the TOP SECRET TEKs used to interconnect operational TRI-TAC switches. Each edition of these keys is effective for three months. Because TRI-TAC switches are normally fielded on an ad hoc basis, most users of these keys must by-pass unused segments to access those that provide required connectivity. Such exposed segments must then be sealed in opaque, tamper-evident, plastic bags; see paragraph (4) below.

NOTE: (U//FOUO) Each edition of USKAT 60501 - 60580 contains one copy each of 80 unique TEKs.

(4) (U//FOUO) **Tamper-Evident Bags** - Based on their experience with use of tape keys that must be retained outside their protective canisters throughout their effective cryptoperiods, each holder should requisition an appropriate number of COMSEC-accountable, 6"x 6", opaque, plastic, tamper-evident bags from the Marketing Group of the NSA Protective Technologies Division (Y26) to meet their projected operational requirements. Since these bags are expensive and have a shelf-life of only about eighteen months, requesting COMSEC custodians/managers should order only those they expect to use within a year.

NOTE: (U//FOUO) Use of the tamper-evident bags requires that each using activity hold an NSA pamphlet, INSPECTION AND HANDLING CRITERIA FOR TAMPER-EVIDENT BAGS, which may be requested from the NSA Y26 Marketing Group at DSN 644-6816 or commercial (301) 688-6816.

ANNEXES:

A - TERMS AND DEFINITIONS
B - KEY TAPE ORDERING GUIDE
C - LOGGING ELECTRONIC KEY TRANSFERS
D - KG-84A/C AND KIV-7/7HS OTAD PROCEDURES
E - KY-57/58/67 OTAD PROCEDURES
F - KYV-5/KY-99/99A/100 OTAD PROCEDURES
G - KY-68 OTAR PROCEDURES
H - KW-46 OTAD PROCEDURES
I - OTAR AND OTAT USING AN/CYZ-10

ANNEX A

TERMS, DEFINITIONS, AND ACRONYMS

Specialized terms used in this document are defined below, and acronyms are expanded.

Term	Definition
automatic remote rekeying (AK)	Procedure to rekey a distant crypto-equipment electronically without specific actions by the receiving terminal operator.
BLACK key	Encrypted key.
cold start	Procedure for initially keying crypto-equipment.
COMSEC account	Administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.
COMSEC custodian	Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding and destruction of COMSEC material assigned to a COMSEC account.
COMSEC emergency	Tactical operational situation, as perceived by the responsible commander, in which the alternative to strict compliance with procedural restrictions affecting use of a COMSEC equipment would be plain text communications.
COMSEC equipment	Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized intercepter and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, crypto-production equipment, and authentication equipment.
COMSEC incident	Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information.
COMSEC manager	Person who manages the COMSEC resources of an organization.
NOTE: Air Force COMSEC managers perform the duties of COMSEC custodians and also manage the COMSEC resources of their COMSEC accounts. Air Force does not have COMSEC custodians.	

controlling authority (CA)	Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.
crypto-equipment	Equipment that embodies a cryptographic logic.
cryptonet	Stations that hold a specific key for use.
cryptoperiod	Time span during which each key setting remains in effect.
frequency hopping	Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications.
key	Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-countermeasures patterns, e.g., frequency hopping or spread spectrum), or for producing other keys.
key encryption key (KEK)	Key that encrypts or decrypts other key for transmission or storage.
manual remote rekeying (MK)	Procedure by which a distant crypto-equipment is rekeyed electronically, with specific actions required by the receiving terminal operator.
net control station (NCS)	Terminal in a secure telecommunications net responsible for distributing key in electronic form to the members of the net.
over-the-air key distribution (OTAD)	Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.
over-the-air key transfer (OTAT)	Electronically distributing key without changing the traffic encryption key used on the secured communications path over which the transfer is accomplished.
over-the-air rekeying (OTAR)	Changing traffic encryption key or transmission security key in remote crypto-equipment by sending new key directly to the remote crypto-equipment over the communications path it secures.
RED key	Unencrypted key.

spread spectrum	Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum.
start-up KEK	Key encryption key held in common by a group of potential communicating entities and used to establish ad hoc tactical networks.
supersession	Scheduled or unscheduled replacement of a COMSEC aid with a different edition.
traffic encryption key (TEK)	Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.
transmission security (TRANSEC)	Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.
transmission security key (TSK)	Key that is used in the control of transmission security processes, such as frequency hopping and spread spectrum.
Acronym	**Expansion**
AIRTERM	Air Terminal (ANDVT)
AK	Automatic Rekeying
ANDVT	Advanced Narrowband Digital Voice Terminal
BAV	Broadcast Area Variable (KW-46)
BCS	Broadcast Control Station (KW-46)
CA	Controlling Authority
CMCS	COMSEC Material Control System
COMSEC	Communications Security
CT3	Common Tier 3 (DTD)
CV	Community Variable (KW-46)
DSN	Defense Switched Network
DTD	Data Transfer Device (EKMS)
EKMS	Electronic Key Management System
ERF	Electronic Remote Fill (SINCGARS)

GENSER	General Service
ICP	Intertheater COMSEC Package
JFILL	Joint Fill (JTIDS)
JTIDS	Joint Tactical Information Distribution System
KEK	Key Encryption Key
KP	Key Processor (EKMS)
KVG	Key Variable Generator (KG-83, KGX-93, KGX-93A)
LMD	Local Management Device (EKMS)
LVT	Low Volume Terminal (MIDS)
MIDS	Multifunctional Information Distribution System
MK	Manual Rekeying
MK/RV	Manual Rekeying/Receive Variable
MSE	Mobile Subscriber Equipment
NATO	North Atlantic Treaty Organization
NCS	Net Control Station
NCTAMS	Naval Computer and Telecommunications Master Station
NDA	National Distribution Authority
NSA	National Security Agency
OS	Outstation
OTAD	Over-the-Air Key Distribution
OTAR	Over-the-Air Rekeying
OTAT	Over-the-Air Key Transfer
P-T-P	Point-to-Point
RS	Receiving Station (KW-46)
SCI	Sensitive Compartmented Information
SI	Special Intelligence
SINCGARS	Single Channel Ground / Air Radio System
STE	Secure Terminal Equipment
STU	Secure Telephone Unit
TACTERM	Tactical Terminal (ANDVT)

TEK	Traffic Encryption Key
TPI	Two-person Integrity
TrKEK	Transfer Key Encryption Key (DTD)
TRANSEC	Transmission Security
TSK	Transmission Security Key
USCG	United States Coast Guard
USN	United States Navy
UV	Unique Variable (KW-46)

ANNEX B

(U) KEY TAPE ORDERING GUIDE

1. (U//FOUO) **GENERAL GUIDANCE** - Key Encryption Key (KEK) and start-up KEK are normally produced in punched tape form, but TEK (including OTAR TEK) required by tactical forces should be produced as close to the using locations and as near to the time of use as is feasible. If a NCS has access to a KG-83/KGX-93/KGX-93A KVG or to an EKMS terminal or uses an equipment such as the KY-57 that is authorized to produce its own TEK, needed TEK and OTAR TEK should be field generated. TEK in tape form should only be used when field generation is not a viable alternative.

2. (U) **PURPOSE** - This annex is provides guidance to assist CAs in ordering KEK, start-up KEK, TEK, and OTAR TEK, in tape form, when field generation is not a viable alternative.

3. (U//FOUO) **LONG TITLE** - The CA who requisitions tape key must assign a descriptive long title to each new tape key. Long titles may contain up to 100 characters, to identify the user community, crypto system (where appropriate), and purpose of the key. Long titles, e.g., USPACOM START-UP KEK, are not printed on the associated key tapes, but provide useful information when entered into NSA and Service CMCS data bases.

4. (U) **ORDERING TAPE TEK**

a. (U//FOUO) **Uses** - For nets/circuits that distribute TEK via OTAR, tape TEK serves two purposes. At NCSs that derive TEK from certified KG-83/KGX-93s of EKMS terminals, irregularly superseded tape TEK serves as emergency back-up, in case of a KVG or EKMS failure. At NCSs that do not use field-generated TEK, tape TEK is required. Tape TEK associated with OTAR is not dedicated to any specific net, circuit, or COMSEC equipment. In that application, a short title of appropriately classified key tape can serve as the source of OTAR TEK for any or all nets and circuits that are controlled by a NCS.

b. (U//FOUO) **Format** - Tape TEK intended for use on nets/circuits that distribute TEK via OTAR is produced in the "V_" format, indicating that each canister contains 62 segments. The second letter of the digraph identifies the cryptoperiod, which may vary with specific uses.

c. (U//FOUO) **Copy Count** - Only one copy is produced of each edition of tape TEK intended for use on nets/circuits that distribute TEK via OTAR, since the using NCS is the only holder. Each alternate NCS should hold its own short title(s) of one-copy tape TEK.

d. (U//FOUO) **Supersession** - At the discretion of the CA, tape TEK may be resupplied on a regular or irregular basis.

(1) (U//FOUO) **Irregular** - In most tactical applications, the consumption rate for tape TEK is not accurately predictable. For example, a commander who has been designated as a possible NCS for a particular start-up KEK may not serve in that capacity for long periods, or tape TEK held as back-up for a stand-alone (non-TRI- TAC) KG-83 may never be used. In applications of this nature, CAs should order reasonable quantities of tape OTAR TEK, each edition of.which is

superseded irregularly, and should reorder follow-on editions as needed, allowing four months for production and delivery. The recommended procurement strategy is to requisition as many editions of a single short title of tape OTAR TEK as may be required for each using NCS or alternate NCS. Where tape OTAR TEK is held only as back-up, the recommended stock level is one month's worth of expected use. That period should be long enough to requisition and obtain a replacement KVG or to repair an EKMS terminal.

(2) (U//FOUO) **Regular** - In applications where its use rate can be predicted, the number of 62-segment TEK tape canisters required to meet a NCS's requirements and the schedule on which they are resupplied are inter-related. Continuing resupply requires that the CA adjust the number of short titles and their supersession schedules to ensure that the required volume of tape TEK is received. For example, if a NCS expects to use 150 segments of tape TEK per month, the CA should order three, monthly-superseded short titles.

5. (U) **ORDERING TAPE START-UP KEK**

a. (U//FOUO) **Use** - Start-up KEK tape supports the establishment of temporary tactical nets and circuits secured by KY-57/58/67, KYV-5/KY-99, or KG-84/KIV-7 equipment. Any military commander may order a start-up KEK tape for use by an identified community of potential users. Requisitioners should allow four months for production and distribution.

b. (U//FOUO) **Format** - Start-up KEK tape is produced in the “VA” format (62 segments - daily crypto-period).

c. (U//FOUO) **Copy Count** - The copy count in which a start-up KEK tape is requisitioned should provide for the expected number of holders and a reasonable number of spare copies to accommodate unplanned additions to the cryptonet. The CA must designate where spare copies are to be held. The U.S. NDA does not hold spare (uncommitted) copies of operational key.

d. (U//FOUO) **Supersession** - Each edition of start-up KEK tape is regularly superseded at two-month intervals.

6. (U//FOUO) **ORDERING TAPE KEK** - Where physical distribution in keyed fill devices is operationally viable, KEK should be field-generated. However, since many tactical environments require use of tape KEK, guidance for ordering tape KEK follows.

a. (U//FOUO) **Use** - Tape KEK, rather than tape start-up KEK, should be used on KG-84/KIV-7, KY-57/58/67, and KYV-5/KY-99 secured nets and circuits that exist on a continuing basis and that distribute TEK via OTAR.

b. (U//FOUO) **Forma**t - Tape KEK (except that used with KW-46) is normally produced in the “GF” (16 segments - three month cryptoperiod), but KEK may be ordered in the “AF” or “VF” formats (31 and 62 segments, respectively, for use on nets/circuits that experience numerous cold starts. At least four segments per edition are used each year, and the remaining segments are available for cold starts.

c. (U//FOUO) **Copy Count** - In point-to-point applications and nets that use a unique KEK for each OS, that is, nets that OTAR sequentially, the copy count for each edition of tape KEK is two. In

multi-station nets that OTAR simultaneously, the copy count corresponds to the number of net members. The CA may order a few extra copies, to accommodate possible future cryptonet expansion and must designate where such extra copies will be held. The U.S. NDA does not hold spare (uncommitted) copies of operational key.

d. (U//FOUO) **Supersession** - Each edition of tape KEK associated with continuing nets and circuits is superseded annually. Tape KEK associated with contingency applications may be requisitioned with irregular supersession, but this places the burden of ensuring continuing resupply on the CA. In either case, four months should be allowed for production and distribution of tape KEK.

7. (U) **ORDERING KW-46 OTAT TAPE KEK**

a. (U//FOUO) **Use** - Navy, Coast Guard, and NATO KW-46 secured broadcasts that are used to transfer key to forces afloat via OTAT require tape KEKs.

b. (U//FOUO) **Format** - KW-46 tape KEK is produced in the "DC" format (5 copies each of 6 segments - monthly cryptoperiod).

c. (U//FOUO) **Copy Count** - Each ship or station required to copy a Navy or Coast Guard broadcast that transfers key via OTAT must hold at least one copy of the tape KEK used with that broadcast.

d. (U//FOUO) **Supersession** - Each edition of KW-46 tape KEK is superseded semi-annually.

8. (U//FOUO) **FUTURE EDITION PROVISIONING** - CAs should ensure that user COMSEC accounts hold at least one future edition of tape KEK and tape start-up KEK.

9. (U) **TAPE KEY ORDERING CHART** - The foregoing information relating to OTAR key, other than KW-46 tape key, is recapitulated in chart form for the convenience of CAs.

NOTE: (U) Substantive entries in the following table are UNCLASSIFIED//FOR OFFICIAL USE ONLY.

ORDERING GUIDE FOR OTAR KEY

TYPE KEY	USE	FORMAT	COPY COUNT	EDITION SUPER.	RESUPPLY STRATEGY
OTAR TEK	Back-up for KVG or EKMS	VA, VB, or VC	1	Irregular	1 short title per NCS - order editions as needed.
OTAR TEK	Primary source (not field generated)	VA, VB, or VC	1	Irregular	Adjust number of short titles and supersessions.
Start-up KEK	Temporary OTAR nets & circuits	VA	1/net mem. & spares	Regular every 2 months	Users hold one future edition.

KEK	Continuing P-T-P circuits	GF	2	Regular yearly	Users hold one future edition.
KEK	Continuing nets that OTAR simultaneously	GF	1/net mem. & spares	Regular yearly	Users hold one future edition.
KEK	Continuing nets that OTAR sequentially	GF	2	Regular yearly	Users hold one future edition.
KEK	Contingency OTAR nets & circuits	GF, AF or VF	1/net mem. & spares	Irregular	Users hold one future edition.

NOTE: First letter of format digraph expresses key tape segment count per canister. “A” = 1 copy each of 31 unique segments, “G” = 1 copy each of 16 unique segments, “V” = 1 copy each of 62 unique segments. Second letter of format digraph expresses cryptoperiod. “A” = Daily, “B” = Weekly, “C” = Monthly, “F” = Quarterly

ANNEX C

(U) LOGGING ELECTRONIC KEY TRANSFERS

1. (U//FOUO) **CONTROLLING AUTHORITY (CA) RESPONSIBILITIES** - The COMSEC Material Control System is not involved in accounting for electronic key, that is, key converted from tape for OTAD or that is field generated. Each commander who directs field generation of a key becomes its Controlling Authority (CA) and is responsible for identifying and tracking it. Additionally, when the electrical equivalent of a tape key is distributed electronically by other than its CA to units that do not normally hold it, the CA must be advised and must record such distribution.

2. (U//FOUO) **RECORD KEEPING** - Activities that generate/convert, transmit, relay, and receive electronic key must track these functions until each key has served its purpose. Shown below is a suggested form for recording production and handling of electronic key in tactical applications. Activities responsible for keeping such records may use any other form(s) or accounting means that fulfill their operational requirements, for example, DA Form 5251-1 (CONAUTH Key Management Worksheet) or DA Form 5251-1-R (CMCS Key Management Worksheet).

(Classification) (Logging Command) (Year)

(U) ELECTRONIC KEY GENERATION AND DISTRIBUTION LOG

ID & Type	CA	Eff. Pd.	Cl.	To/At	From/At
0752ID210 KY-57/58[a]	52ID	1-7 AUG	S	1st BDE/52ID 311500Z JUL	
0752ID210 KY-57/58[b]	52ID	1-7 AUG	S	.	521ID 311500Z JUL
0752ID210 KY-57/58[c]	52ID	1-7 AUG	S	1st BDE/52ID 311500Z JUL.	2nd Bde/ 52ID 311500Z JUL
U6343D03 KG-84A[d]	HQ USAFE	10-16 NOV	C	2100CS 091320Z NOV	
0752ID210 KY-57/57[e]	52ID	1-7 AUG	S	3d Bde/52ID 2281399Z JUL	
U634D03 KG-84A[f]	HQ USAFE	10-16 NOV	C	2100CS 081210Z NOV	

a. Typical entry for sender of field-generated key.
b. Typical entry for receiver of field-generated key.
c. Typical entry for relayer of field-generated key.
d. Typical entry of sender for electronic key converted from tape.
e. Typical entry for physical issuer of field-generated key.
f. Typical entry for physical issuer of electronic key converted from tape.

(Classification)

THIS PAGE IS INTENTIONALLY BLANK

ANNEX D

(U) KG-84A/C AND KIV-7/7HS OTAD PROCEDURES

1. (U//FOUO) **INTRODUCTION -** The KG-84A/C and KIV-7/7HS provide for encryption of teletypewriter and digital data. They operate in full duplex, half duplex, and simplex modes and may be used on point-to-point circuits and multi-station nets. When controlled by a DTD or a KYX-15, a KG-84 or KIV-7 is capable of distributing electronic key via 0TAR or OTAT. A KIV-7 can also perform OTAR functions using only a KOI-18 tape reader; see paragraph 4.b. on page D-3 below.

NOTE: (U) Throughout the remainder of this Annex, KG-84A and KG-84C equipment is referred to as "KG-84", and KIV-7 and KIV-7HS equipment is referred to as "KIV-7".

2. (U) **PURPOSE AND SCOPE -** This annex provides standard procedures for initially keying (cold starting) the KG-84 and KIV-7 and for accomplishing point-to-point circuit OTAR, net OTAR, OTAT with common KEK or start-up KEK, and OTAT with multiple KEKs.

NOTE: (U) Although the tape key fill routines stated below specify use of the KOI-18 tape reader, key may also be filled into KG-84 and KIV-7 equipment from KYK-13 and KYX-15 common fill devices and DTDs.

CAUTION: (U) Prior to cold starting KG-84/KIV-7 equipment or performing OTAR or OTAT procedures, ensure that any fill device to be used is functioning properly and has sufficient battery energy to complete the operation.

NOTE: (U) Substantive notes and procedural statements in this Annex are UNCLASSIFIED// FOR OFFICIAL USE ONLY. Innocuous statements, such as "wait" and "communicate normally" are UNCLASSIFIED.

3. (U) **KG-84 AND KIV-7 COLD START** - Cold starting of KG-84/KIV-7 point-to-point circuits and multi-station nets should only be required when the circuit/net is established or when a COMSEC equipment fails.

CAUTION: (U//FOUO) Cold starting KG-84/KIV-7 nets/circuits without updating the KEK that is being used as a temporary OTAR TEK (i.e., without performing step 2 in paragraphs 3.a. or 3.b. or step 3 in paragraph 3.c.) is a reportable cryptographic COMSEC incident.

a. (U//FOUO) **Cold Starting Point-to-Point Circuits**

NET CONTROL STATION	OUTSTATION
1. Prior to circuit activation, load appropriate segment of KEK or start-up KEK in KG-84/KIV-7 U and X1 fill positions.	Prior to circuit activation, load appropriate segment of KEK or start-up KEK in KG-84/KIV-7 U and X1 fill positions.
2. Update key in NCS KG-84/KIV-7 X1 fill position.	Update key in OS KG-84/KIV-7 X1 fill position.

NET CONTROL STATION	OUTSTATION
3. Replace key in NCS and OS KG-84/KIV-7 X1 fill position by MK OTAR.	Wait.

b. (U//FOUO) **Cold Starting Multi-station Nets with Start-up KEK or Common KEK**

NET CONTROL STATION	OUTSTATION
1. Prior to net activation, load appropriate segment of KEK or start-up KEK in KG-84/KIV-7 U and X1 fill positions.	Prior to net activation, load appropriate segment of KEK or start-up KEK in KG-84/ KIV-7 U and X1 fill positions.
2. Update key in NCS KG-84/KIV-7 X1 fill position.	Update key in OS KG-84/KIV-7 X1 fill position.
3. Replace key in NCS and OS KG-84/KIV-7 X1 fill position by AK OTAR.	Wait.

c. (U//FOUO) **Cold Starting Multi-station Nets with OS-unique KEK**

NET CONTROL STATION	OUTSTATION
1. Prior to net activation, load designated segment of each OS's KEK in KYX-15 fill position 16 and sequentially lower.	Prior to net activation, load designated segment of KEK in KG-84/KIV-7 U and X1 fill positions.
2. Load KEK for first OS to be OTARed in KG-84 or KIV-7 U and X1 fill positions.	Wait.
3. Update key in NCS KG-84/KIV-7 X1 fill position.	Update key in OS KG-84/KIV-7 X1 fill position.
4. Replace key in KG-84/KIV-7 X1fill position of first OS to be rekeyed via AK OTAR.	Wait.
5. Repeat steps 1 thru 4 for next OS to be rekeyed using its KEK.	OS being OTARed performs steps 1 thru 4.
6. Repeat step 5 for each other OS to be OTARed.	Repeat step 5 for each other OS to be OTARed

4. (U//FOUO) **KG-84 AND KIV-7 POINT-TO-POINT OTAR (MK) -** Only the routine prescribed in paragraph a. below is available for performing KG-84 MK OTAR. However, KIV-7 MK OTAR may be done by either the “regular” routine stated in paragraph a. or the “front panel” routine that is prescribed in paragraph b.

NOTE: (U//FOUO) To accomplish OTAR on point-to-point circuit, both KG-84 or KIV-7 must hold identical TEK and KEK, and the circuit must be active.

NOTE: (U//FOUO) Referring to KG-84/KIV-7 point-to-point circuit OTAR procedures as "MK" is semantically inconsistent, because the process is accomplished without actions by receiving terminal operators and is, therefor, "non-cooperative".

a. (U//FOUO) **Regular KG-84 and KIV-7 MK OTAR** - The NCS executes the following steps:

1. If tape TEK is used, connect KOI-18 to KYX-15.
2. Set KYX-15 MODE switch on "LD".
3. Turn "ON" empty KYX-15 toggle switch to store new TEK. **NOTE**: TEK is stored in lower numbered toggle switches.
4. Press and release KYX-15 INITIATE button.
5. Within 20 seconds, pull TEK tape thru KOI-18. **NOTE**: KYX-15 PARITY light flashes.
6. Turn KYX-15 MODE switch to "OFF/CK".
7. Disconnect KOI-18 from KYX-15.
8. Notify OS to expect OTAR and to refrain from transmitting until it is complete.
9. Connect KYX-15 to KG-84/KIV-7.
10. Turn KYX-15 MODE switch to "MK".
11. Turn "ON" KYX-15 toggle switch for new TEK.
12. Press KYK-15 INITIATE button. **NOTE:** If the KG-84/KIV 7 DATA LENGTH switch is set to "SYNCHRONOUS DATA", the FULL OPR and RCY RDY lights blink, indicating an out of sync condition and that a successful OTAR has occurred. If the KG-84/KIV-7 DATA LENGTH switch is set to "ASYNCHRONOUS DATA", those lights keep cycling, indicating an out of sync condition. If these indicators are not observed and the circuit remains in crypto synchronization, repeat steps 11 and 12.
13. Turn KG-84/KIV-7 MODE switch to "V--X".
14. Raise and release KG-84/KIV-7 INITIATE/IND TEST switch.
15. Turn KG-84/KIV-7 MODE switch to "OPR".
16. Turn KYX-15 MODE switch to "Z SEL".
17. Press and release KYX-15 INITIATE button.
18. Turn KYX-15 MODE switch to "OFF/CK".

19. Turn “OFF” KYX-15 toggle switch for TEK.
20 Disconnect KYX-15 from KG-84/KIV-7.
21. Log date and time of OTAR and zeroization of TEK.

b. (U//FOUO) **KIV-7 Front Panel MK OTAR -** This is an optional procedure for P-T-P circuits that allows a NCS using a KIV-7 (even if the OS uses a KG-84) to pre-load up to ten OTAR TEKs and to perform an OTAR when a KYX-15 or AN/CYZ-10 is not available. To perform a KIV-7 front panel MK OTAR using punched paper tape OTAR TEK that is drawn thru a KOI-18, the NCS uses steps 1-3 and 10-32. To perform the operation using electronic OTAR TEK that is stored in a KYK-13, the NCS uses steps 1 and 4-32.

NOTE: (U//FOUO) No KIV-7 front panel **AK OTAR** procedure has been developed.

1. On KIV-7, press “ONLINE” to go offline.
2. If tape OTAR TEK is used, connect KOI-18 to KIV-7.
3. Pull OTAR TEK tape segment thru KOI-18, and skip to step 10.
4. If electronic OTAR TEK is used, connect KYK-13 containing new OTAR TEK to KIV-7.
5. Turn lower KYK-13 switch to position of new OTAR TEK.
6. Turn upper KYK-13 switch to “ON”.
7. Scroll KIV-7 menu until display reads “LOAD” & press INITIATE button.
8. Scroll KIV-7 menu to select X10 fill position. **NOTE:** Any empty X fill position will work, but for remainder of these procedures, X10 will be used as location of OTAR TEK, and working TEK will be in fill position X01. **NOTE:** KIV-7 display reads “=LD X10”.
9. Press INITIATE button. **NOTE:** If key loading was successful, KIV-7 display reads “LoadGood”. If display reads “LoadFail”, check KYK-13 for connection error and repeat steps 4 - 9.
10. Press KIV-7 ONLINE button to establish communications. **NOTE:** KIV-7 display reads “FDX TR”.
11. Scroll KIV-7 menu to “TXrekey” & press INITIATE button.

12. Scroll KIV-7 menu to “=KEY X10” & press INITIATE button. **NOTE:** KIV-7 display reads “REKEYING” for few seconds, the “Snd Good”, then “FDX”, then FDX TR”. **NOTE:** KIV-7 ONLINE light flashes and audio tones cycle in pattern, indicating that KIV-7 is attempting to establish communications using old OTAR TEK.
13. Press KIV-7 ONLINE button until display reads “OFF-LINE”.
14. Scroll KIV-7 menu to “SEL KEY” & press INITIATE button. **NOTE:** KIV-7 display reads “REKEYING”, then “Snd Good” and then “FDX>
15. Scroll KIV-7 menu to “-KEY X10” & press INITIATE button. **NOTE:** KIV-7 display reads “Key Good”.
16. Press KIV-7 ONLINE button. **NOTE:** KIV-7 should establish communications. If OTAR is successful, KIV-7 display reads “FDX TR”. Then go to step 22.
17. If OTAR not successful, press KIV-7 ONLINE button until display reads “OFFLINE”.
18. Scroll KIV-7 menu to “-SELKEY” & press INITIATE button.
19. Scroll KIV-7 menu to select key “=KEY X01.
20. Press KIV-7 ONLINE button. **NOTE:** KIV-7 attempts to establish communications, and display reads “FDX TR” constantly.
21. Repeat steps 10-16.
22. Press KIV-7 ONLINE button until display reads “OFFLINE”.
23. Scroll KIV-7 menu to “-SEL KEY” & press INITIATE button.
24. Scroll KIV-7 menu to fill position “-KEY X01”& press INITIATE button.
25. Scroll KIV-7 to “Return” & press INITIATE button.
26. Scroll KIV-7 menu to “-XFR V---X” & press INITIATE button.
27. Scroll KIV-7 menu to “-V--- X01”. & press INITIATE button. **NOTE:** KIV-7 display reads “V---X Good”.
28. Press KIV-7 ONLINE button. **NOTE:** KIV-7 establishes communications.

29. Press KIV-7 ONLINE button until display reads “OFF-LINE”>
30. Scroll KIV-7 menu to “-ZEROIZE” & PRESS initiate button.
31. Scroll KIV-7 menu to “=ZEO X10” & press INITIATE button. **NOTE:** KIV-7 display flashes “ZEROIZED”.
32. Press KIV-7 ONLINE button. **NOTE:** KIV-7 establishes communications with OS. OTAR process is complete.

5. (U//FOUO) **KG-84 AND KIV-7 NET AK OTAR**

a. (U//FOUO) **Allocating Net KEKs -** If more than one KEK is used in a net, OTAR must be accomplished by the longer, sequential method, but if a common KEK or start-up KEK is assigned for all net OSs, the shorter, simultaneous method can be used. In either case, the effective net TEK must be held in the NCS and OS KG-84/KIV-7 equipment, and the updated version of each OS KEK or the updated net KEK or start-up KEK, must be retained in the NCS KYX-15 between OTAR cycles.

NOTE: (U//FOUO) When storing KEKs to support AK OTAR, the general prohibition against holding key in fill devices does not apply. When performing OTAR with a KYX-15, up to fifteen OSs can be rekeyed in sequence, without changing the KYX-15. If a net has more than fifteen active OSs, the OTAR cycle must be broken into two or more 15-OS groups. Under that circumstance, the NCS should consider using the simultaneous OTAR routine.

b**. (U//FOUO) KG-84 and KIV-7 AK OTAR -** The NCS executes the following steps:

NOTE: (U) Like the KG-84/KIV-7 point-to-point OTAR process, the KG-84/ KIV-7 net OTAR process is “non-cooperative”.

NOTE: (U//FOUO) No KIV-7 Front Panel AK OTAR procedure has been developed.

1. Load new TEK into KYX-15 fill position 1. **NOTE:** NCS KYX-15 must now hold new TEK in fill position 1 and current KEK for each OS or group of OSs in fill positions 16 - 2.
2. Poll net and notify OSs to be ready for an OTAR and to refrain from transmitting until OTAR is complete.
3. Turn KYX-15 MODE switch to “AK”.
4. Turn “ON” KYX-15 toggle switches for KEK of each OS to be rekeyed.
5. Turn “ON” KYX-15 toggle switch for TEK.

6. Press and release KYX-15 INITIATE button. **NOTE:** At conclusion of each AK operation, KG-84/KIV-7 XMT RDY and RCV RDY lights flash.
7. Turn “OFF” all KYX-15 toggle switches.
8. Turn KYX-15 MODE switch to “OFF/CK”.
9. Turn KG-84/KIV-7 VAR SEL switch to vacant X fill position.
10. Turn KG-84/KIV-7 MODE switch to “V---X”.
11. Raise and release KG-84/KIV-7 INITIATE/IND switch.
12. Turn KG-84/KIV-7 MODE switch to “OPERATE”.
13. Poll net. **NOTE:** Only OSs that were rekeyed can respond.
14. If there are stragglers who failed to respond, set KG-84/KIV-7 VAR SEL switch to position of old TEK.
15. Call straggler OSs.
16. Turn “ON” KYX-15 toggle switches for straggler station KEKs.
17. Turn KYX-15 MODE switch to “AK”.
18. Repeat steps 5. thru 12.
19. When all stragglers have been rekeyed, call net and authorize return to regular communications.
20. Set KYX-15 MODE switch to “VU”.
21. Turn “ON” KYX-15 toggle switches for all OX KEKs. **CAUTION:** Do not perform step 22. until all authorized OSs have been rekeyed.
22. Push KYX-15 INITIATE button.
23. Turn “OFF” KYX-15 toggle switches for all OS KEKs.
24. Turn “ON” KYX-15 toggle switch for new TEK
25. Turn KYX-15 MODE switch to “Z SEL”.
26. Press and release KYX-15 INITIATE button.
27. Disconnect KYX-15 from KG-84/KIV-7.
28. Record date / time of OTAR cycle, note any OSs dropped from or added to net, log fact that all net KEKs have been updated and TEK zeroized from KYX-15, and note KG-84/KIV-7 location of net TEK.

6. (U//FOUO) **KG-84 AND KIV-7 OTAT** - Depending on how KEK is assigned within a KG-84 or KIV-7 secured net, OTAT may be accomplished either sequentially or simultaneously. In nets that use common KEK or start-up KEK, OTAT is done by the simultaneous “MK/RV” procedure, and in nets that use multiple KEKs, OTAT is done by the sequential “MK/RV” procedure. Both of these routines are cooperative, in that they require specific actions by OS operators. With either routine, each OS receiving key must be able to communicate securely with the NCS and must hold KYX-15 or AN/CYZ-10 for extracting the received key.

a. (U//FOUO) **OTAT with Common KEK or Start-up KEK (MK/RV)** - The following procedural steps are required to accomplish simultaneous OTAT on nets in which all OSs hold the same KEK:

NOTE: (U) AN/CYZ-10 may be used in place of KYX-15.

NET CONTROL STATION	OUTSTATION
1. Connect KYX-15 containing TEK to be transferred to KG-84/KIV-7.	Communicate normally.
2. Turn "ON" KYX-15 toggle switch of key to be transferred.	Communicate normally.
3. Poll net, notify OSs to prepare for MK/RV OTAT, and identify tag assigned to key to be transferred.	Communicate normally.
4. Direct OSs to turn KG-84/KIV-7 COMM MODE SWITCH to SIMPLEX mode, to acknowledge, and then to refrain from transmitting until OTAT routine is complete.	Respond in polling order and set KG-84/ KIV-7 COMM MODE switch to SIMPLE.X,
5. Turn KG-84/KIV-7 COMM MODE switch to SIMPLEX.	Wait.
6. Direct OSs to connect KYX-15 to KG-84/KIV-7 and turn "ON" KYX-15 toggle switch for vacant fill position	Connect KYX-15 to KG-84/KIV-7 and turn “ON” KYX-15 toggle switch for vacant fill position.
7. Direct OSs to turn KYX-15 MODE switch to "RV" and to push KYX-15 INITIATE button.	Turn KYX-15 MODE switch to "RV" and push INITIATE button.
8. Turn KYX-15 MODE switch to "MK".	Wait.
9. After 20 seconds, press KYX-15 INITIATE button.	After KYX-15 PARITY light blinks once, set KYX-15 MODE switch to "OFF/CK".
10. Wait.	Push KYX-15 INITIATE button and watch for PARITY light to and watch for PARITY light to blink.

NET CONTROL STATION	OUTSTATION
11. Wait.	Turn "OFF" KYX-15 toggle switch for received key.
12. Poll net and query whether OTAT was successful.	Respond in polling order and advise whether OTAT was successful
13. Call net and direct return to normal communications.	Communicate normally.
14. Turn "OFF" all KYX-15 toggle switches.	Turn "OFF" all toggle switches.
15. Turn KYX-15 MODE switch to “OFF/CK”.	Turn KYX-15 MODE switch to "OFF/CK".
16. Disconnect KYX-15 from KG-84/KIV-7.	Disconnect KYX-15 from KG-84/KIV-7.
17. Log OTAT date, time, and tags of keys transferred.	Log OTAT date, time, tags of keys received and sender.

b. (U//FOUO) **OTAT with Multiple KEKs (MK/RV)** - The following procedural steps are required to accomplish sequential OTAT on nets that use multiple KEK:

NET CONTROL STATION	OUTSTATION
1. Connect KYX-15 containing key transferred and KEKs of OSs that are to receive key to KG-84/ KIV-7.	Communicate normally.
2. Turn “ON” KYX-15 toggle switch of key to be transferred.	Communicate normally.
3. Poll net, notify OSs to prepare for OTAT, and direct them to refrain from transmitting until OTAT routine complete.	Respond in polling order, then refrain from transmitting until OTAT routine is complete.
4. Load KEK of first OS to receive key to KG-84/ KIV-7.	Wait.
5. Alert OS that will receive key to standby for MK/ RV OTAT,	Addressed OS responds. Other OSs refrain from transmitting.
6. Call receiving OS and advise “tag” of key to be transmitted.	Record tag of key to be received.
7. Direct receiving OS to connect KYX-15 to KG-84/KIV-7 and to turn “ON” KYX-15 toggle switch for vacant fill position.	Connect KYX-15 to KG-84/KIV-7 and turn “ON” KYX-15 toggle switch for vacant fill position.
8. Direct OS to turn KYX-15 MODE switch to “RV” and to push KYX-15 INITIATE button.	Turn KYX-15 MODER switch to “RV” and push INITIATE button.
9. Turn KYX-15 MODE switch to “MK”.	Wait.

NET CONTROL STATION	OUTSTATION
10. After 20 seconds, press KYX-15 INITIATE button.	After KYX_15 PARITY light blinks once, set KYX-15 MODE switch to “OFF/CK”.
11. Wait.	Push KYX-15 INITIATE button, and watch for PARITY light to blink.
12. Wait.	Turn “OFF” KYX-15 toggle switch for received key.
13. Call receiving OS and query whether OTAT was received.	Respond, and advise NCS whether OTAT was successful.
14. Repeat steps 6. thru 13. for each additional key to be transferred.	Repeat steps 6. thru 13., as directed by NCS.
15. Repeat steps 4. thru 14. to transfer keys to other OSs.	Other OSs repeat steps 4. thru 14., as directed by NCS.
16. Call net and direct return to normal communications.	Communicate normally.
17. Turn “OFF” all KYX-15 toggle switches.	Turn “OFF” all KYX-15 toggle switches.
18. Turn KYX-15 MODE switch to “OFF/CK”.	Turn KYX-15 MODE switch to “OFF/CK”.
19. Disconnect KYX-15 from KG-84/KIV-17.	Disconnect KYX-15 from KG-84/KIV-7.
20. Log OTAT date, time, tags of transferred keys, and recipients.	Log OTAT date, time, tags of received keys, and sender.

ANNEX E

(U) KY-57/58/67 OTAD PROCEDURES

1.(U//FOUO) **INTRODUCTION** - The KY-57/58/67 family of tactical secure voice equipment includes the remotely controlled KY-58 that is normally installed in ships, aircraft, vehicles, and fixed locations, the manpack KY-57, and the KY-67 radio/COMSEC equipment that is normally used in U.S. Marine Corps tanks. These three COMSEC equipment types are functionally similar.

2. (U//FOUO) **PURPOSE AND SCOPE** - This annex provides standard procedures for initially keying (cold starting) KY-57/58/67 equipment, for generating key, and for accomplishing OTAR and OTAT on multi-station nets and point-to-point circuits.

NOTE: Although the tape key fill routines stated below specify use of the KOI-18 tape reader, key may also be filled into KY-57/58/67 equipment from KYK-13 and KYX-15 common fill devices and AN/CYZ-10 data transfer devices.

CAUTION: Prior to cold starting KY-57/58/67 equipment or performing OTAR or OTAT procedures, ensure that any fill device to be used is functioning properly and has sufficient battery energy to complete the operation.

3. (U) **KY-57/58/67 COLD START**

a. (U//FOUO) **Using Start-up KEK or Common KEK** - To cold start a KY-57/58/67 secured net or circuit that is being established with start-up KEK or that uses common KEK held by all OSs, use the following steps:

NET CONTROL STATION	OUTSTATION
1. Prior to net activation time, load designated segment of KEK or start-up KEK in KY-57/58/67 fill positions 1 and 6.	Prior to net activation time, load designated KEK in KY-57/58/67 fill positions 1 and 6.
2. Update key in KY-57/58/67 fill position 1.	Update key in KY-57/58/67 fill position 1.
3. Perform an AK OTAR to replace key in fill position 1.	Wait.

NOTE: (U//FOUO) Failure to perform step 2 is a reportable COMSEC incident.

b. (U//FOUO) **Using Multiple KEKs** - To cold start a KY-57/58/67 secured net that uses a unique KEK for each OS or a combination of OS-unique and common KEKs, use the following steps:

NOTE: In a mixed environment, each KEK held by a group of OSs is treated like a separate OS-unique KEK.

NOTE: Failure to perform step 2. is a reportable COMSEC insecurity.

NET CONTROL STATION	OUTSTATION
1. Prior to net activation time, load designated segment of each OS KEK in KYX-15 fill positions 16 thru 2.	Take no action.
2. Load KEK to be used into KY-57/58/67 fill positions 1 and 6.	Prior to net activation time, load designated segment of KEK ub KY-57/58/67 fill positions 1 and 6.
3. Update key in KY-57/58/67 fill position 1.	Update key in KY-57/58/67 fill position 1.
4. Perform AK OTAR for first OS (or net, if common net KEK is used) to replace key in fill position 1.	Wait.
5. Repeat steps 2 - 4 for other OSs, using their KEKs.	Wait.

NOTE: (U//FOUO) Failure to perform step 3. is a reportable COMSEC insecurity.

4. (U//FOUO) **KY-57/58/67 KEY GENERATION** - To generate key with a KY-57/58/67 equipment, the NCS performs the following steps:

1. Turn "ON" KY-57/58/67 power switch.
2. Set KY-57/58/67 MODE switch to "C".
3. Connect KYX-15 to the KY-57/58/67.
4. Set KYX-15 MODE switch to "VG".
5. Turn "ON" KYX-15 ADDRESS SELECT toggle switch for vacant fill position.
6. Depress KYX-15 INITIATE button. **NOTE**: Beeps are audible in KY-57/58/67 handset and KYX-15 PARITY light goes "ON".
7. Turn "OFF" KYX-15 ADDRESS SELECT toggle switch. **NOTE**: If KEY is being generated for an OTAR TEK, omit step 8.
8. Log identifier given to generated key.
9. Repeat steps 4 through 8 as often as necessary to generate additional required keys.
10. Set KYX-15 MODE switch to "OFF/CK".
11. Disconnect the KYX-15 from KY-57/58/67.

5. (U//FOUO) **KY-57/58/67 AK OTAR** - This procedure is the recommended method for KY-57/58/67 secured nets/circuits. It is used when each net or circuit is established and when the NCS wishes to affect an immediate change of the effective TEK. To accomplish an AK OTAR the NCS performs the following steps:

.

NOTE: (U) The AK OTAR procedure is "non-cooperative", in that it requires no actions by outstation (OS) operators, other than responding to NCS calls.

NOTE: (U//FOUO) OSs must load KEK in KY-57/58/67 fill position 6, and the NCS must store all net KEKs in a KYX-15 or DTD between OTAR cycles.

1. Connect KOI-18 to KYX-15. **NOTE**: Omit steps 1 thru 5, if TEK to be transferred is already in KYX-15.
2. Turn "ON" KYX-15 ADDRESS SELECT toggle switch for vacant fill position numbered lower than that used for KEK (normally 1 for TEK and 16 thru 2 for TEK). **NOTE**: TEK must be stored in lowest numbered fill positions and KEK must be stored in highest numbered fill positions.
3. Set KYX-15 MODE switch to "LD".
4. Press KYX-15 INITIATE button.
5. Within 20 seconds, pull TEK tape thru KOI-18. **NOTE**: KYX-15 PARITY light flashes. (If light fails to flash repeat steps 1 thru 5 or check KOI-18 and KYX-15 for proper operation.)
6. Poll net and notify OSs to standby for AK OTAR and to refrain from transmitting until notified by the NCS. **CAUTION**: Do not proceed until all OSs have responded.
7. Connect KYX-15 to KY-57/58/67.
8. Turn "ON" KYX-15 ADDRESS SELECT toggle switches for OS KEKs.
9. Turn "ON" KYX-15 ADDRESS SELECT toggle switch for TEK to be transferred.
10. Set KYX-15 MODE switch to "AK".
11. Press KYX-15 INITIATE button.
12. Turn "OFF" KYX-15 KEK ADDRESS SELECT toggle switches.
13. Turn KY-57/58/67 KEY FILL switch to fill position 5.

14. Poll net. **NOTE**: Only OSs that received TEK will respond. If all OSs respond, omit steps 15.thru 19.
15. If there are stragglers, turn KY-57/58/67 KEY FILL switch to old TEK fill position.
16. Call straggler OSs.
17. Turn "ON" KYX-15 ADDRESS SELECT toggle switches for straggle OS KEKs.
18. Set KYX-15 MODE switch to "AK".
19. Repeat steps 8 thru 18.
20. When all OSs have responded, poll net and authorize OSs to resume normal operation.
21. Set KYX-15 MODE switch to "OFF/CK".
22. Turn "ON" KYX-15 toggle switches for rekeyed OS KEKs.
23. Turn "OFF" KYX-15 toggle switch for TEK.
24. Set KYX-15 MODE switch to "VU". **CAUTION**: Do not perform step 24 until all authorized OSs have received new TEK.
25. Press and release KYX-15 INITIATE button. **NOTE**: KYX-15 PARITY light blinks.
26. Set KYX-15 MODE switch to "OFF/CK".
27. Turn "OFF" all KYX-15 toggle switches.
28. Disconnect KYX-15 from KY-57/58/67.
29. Record date and time of OTAR cycle, note any OSs dropped from or added to net, log KEK updates, and record KY-57/58/67 fill position number of new TEK.

6. (U//FOUO) **KY-57/58/67 MK OTAR** - This procedure is used when the NCS wishes to transfer net or circuit TEK that will become effective at a future time. To accomplish a KY-57/58/67 MK OTAR, use the following steps:

NOTE: (U//FOUO) The KY-57/58/67 MK OTAR procedure is "cooperative", in that it requires actions by OS operators. In netted applications MK OTAR can be accomplished sequentially, if multiple KEKs are used within a net, or simultaneously, if all OSs hold common KEK. The simultaneous method is attractive for large, slow-speed nets.

NOTE: (U//FOUO) For both NCS and OSs, the KEK in use at the time of an MK OTAR must be loaded in KY-57/58/67 fill position 6. When the sequential MK OTAR method is used, the NCS must store all KEKs in a KYX-15 or DTD between OTAR cycles and must load them, one at a time, into fill position 6 of the KY-57/58/67 being used.

.

NET CONTROL STATION	OUTSTATION
1. Load TEK to be transferred into KYX-15.	Communicate normally.
2. Connect KYX-15 to KY-57/58/67.	Communicate normally.
3. Load KEK being used into KY-57/58/67 fill position 6.	Communicate normally.
4. Poll net and direct OSs to refrain from transmitting until notified by NCS.	Respond in polling order, and load KEK being used into KY-57/58/67 fill position 6 (if not already loaded).
5. Direct receiving OS to prepare for MK OTAR. **CAUTION**: Do not proceed until all OSs have responded.	Acknowledge
6. Turn "ON" KYX-15 toggle switch for TEK to be transferred.	Wait.
7. Direct receiving OS (or net, if simultaneous method is being used) to turn KY-57/58/67 KEY FILL switch to fill position 6 and to acknowledge.	Turn KY-57/58/67 KEY FILL switch to fill position 6, and respond (in polling order, if simultaneous method is being used).
8. Turn KY-57/58/67 KEY FILL switch to fill position 6.	Wait.
9. Set KYX-15 MODE switch to "MK".	Wait.
10 Call receiving OS (or net, if simultaneous method is being used) and direct OS(s) to turn KY-57/58/67 MODE switch to "RV" and KEY FILL switch to vacant fill position.	First turn KT-57/58/67 MODE switch to "RV" and then turn KY-57/58/67 KEY TILL switch to vacant fill position.
11. Wait 10 seconds and press and release KYX-15 INITIATE button.	Wait and listen for beeps in handset.
12. Wait.	Turn KY-57/58/67 MODE switch to "C". If beeps are not heard, wait one minute and turn KEY FILL switch to fill position 6.
13. Wait two seconds and turn KY-57/58/67 KEY FILL switch to fill position 5.	Wait.

NET CONTROL STATION	OUTSTATION
14. Call receiving OS (or net, if simultaneous method is being used. **NOTE**: This brief use of future TEK is authorized and is not a reportable COMSEC incident.	Respond (in polling order, if simultaneous method is being used). **NOTE**: This brief use of future TEK is authorized and is not a reportable COMSEC incident.
15. If sequential method is being used and receiving OS fails to respond, repeat steps 6 thru 13. **NOTE:** Omit step 15 if OS responds.	Perform steps 6. thru 14.
16. If sequential method is being used, repeat steps 5 thru 15, for each other OS to receive key. **NOTE**: If simultaneous method is being used, omit step 15.	Perform steps 5. thru 15.
17. If simultaneous method is being used and any OSs fail to respond, turn KY-57/58/67 KEY FILL switch to fill position 6.	Wait.
18. Call stragglers.	Stragglers respond in polling order.
19. Turn "ON" KYX-15 toggle switch for net KEK.	Wait.
20. Direct stragglers to turn KY-57/58/67 MODE switch to "RV" and KEY FILL switch to vacant fill position.	Stragglers set KY-57/58/67 MODE switch to "RV" and KEY FILL switch to vacant fill position.
21. Wait 10 seconds and press KYX-15 INTIATE button.	Stragglers listen for beeps in handset.
22. Wait.	Stragglers turn KY-57/58/67 MODE switch to "C".
23. Wait 2 seconds and set KY-57/58/67 KEY FILL switch to fill position 5.	Wait.
24. Call stragglers.	Respond in straggler polling order.
25. If any OS fails to respond, repeat steps 19 thru 25. **NOTE**: If there are no stragglers, omit steps 19 thru 24.	Affected stragglers perform steps 19 thru 24.

NET CONTROL STATION	OUTSTATION
26. When all OSs have received transferred TEK, direct OSs to turn KY-57/58/67 KEY FILL switch to effective TEK (not TEK just transferred) and to acknowledge.	Set KY057/58/67 KEY FILL switch to effective TEK and respond in polling order.
27. When all OSs have responded, poll net and authorize return to normal communications.	Respond in polling order, and resume normal communications.
28. Set KYX-15 MODE switch to "OFF/CK".	Communicate normally.
29. Turn "OFF" all KYX-15 toggle switches.	Communicate normally.
30. Disconnect KYX-15 from KY-57/58/67.	Communicate normally.

7. **(U//FOUO) KY-57/58/67 OTAT** - The OTAT procedure is used to transfer TEK from one KYX-15 or DTD to another, via a KY-57/58/67 secured net or circuit. Received TEK can be used on any KY-57/58/67 secured net or circuit and, in COMSEC emergencies, on nets and circuits secured by other COMSEC equipment. In COMSEC emergencies, the OTAT procedure may also be used to transfer KEKs. To accomplish KY-57/58/67 OTAT, use the following steps:

> **NOTE**: (U//FOUO) KY-57/58/67 OTAT is "cooperative", in that it requires action by OS operators. It is possible only when the sending and receiving stations hold common KEK and TEK. In netted applications where multiple OSs hold common KEK, the NCS must identify which OS(s) are supposed to receive the transferred key, but cannot prevent reception by other net stations that hold the KEK.

NET CONTROL STATION	OUTSTATION
1. Verify that KEK to be used is loaded in KYX-15 fill position 6.	Communicate normally.
2. Load key(s) to be transferred in KYX-15, starting with fill position 1.	Communicate normally.
3. Connect KYX-15 to KY-57/58/67.	Communicate normally.
4. Poll net and notify OSs to standby for OTAT and to refrain from transmitting until notified. **CAUTION**: Do not proceed until all OSs have responded.	Respond in polling order.

NET CONTROL STATION	OUTSTATION
5. Direct OSs that will receive key to turn KY-57/58/67 KEY FILL switch to fill position 6 and to connect KYX-15 to KY-57/58/67.	Turn KY-57/58/67 KEY FILL switch to fill position 6 and connect KYX-15 to KY-57/58/67. **NOTE**: If KYX-15 or CYZ-10 is not available, notify NCS.
6. Turn KY-57/58/67 KEY FILL switch to fill position 6	Wait.
7. Turn KYX-15 MODE switch to	Wait.
8. Turn "ON" KYX-15 ADDRESS SELECT toggle switch to key to be passed.	Wait.
9. Record tag of key to be transferred.	Wait.
10. Pass tag for key to be passed to receiving OSs and direct them to acknowledge.	Receiving OSs record tag of key to be passed, and respond in polling order.
11. Direct receiving OSs to select KYX-15 fill position to receive transferred key, to turn KYX-15 MODE switch to "RV", and to acknowledge.	Turn "ON" selected KYX-15 ADDRESS SELECT toggle switch, turn KYX-15 MODE switch to "RV", and respond in polling order.
12. Direct receiving OSs to press and release KYX-15 INITIATE button.	Press and release KYX-15 INITIATE button. **NOTE**: Beeps are audible in headset/handset and KYX-15 PARITY light blinks.
13. Press and release KYX-15 INITIAT button.	Wait.
14. Call receiving OSs using KEK (in KY-57/58/67 fill position 6).	Respond in polling order.
15. Direct receiving OSs to load received key into KY-57/58/67 fill position 5.	Load received key into KY-57/58/67 fill position 5.
16. Turn KY-57/58/67 KEY FILL switch to fill position 5.	Wait.
17. Call receiving OSs using transmitted key.	Respond in polling order. **NOTE**: If not called by NCS in one minute, turn KY-57/58/67 KEY FILL switch to fill position 6 and wait.

NET CONTROL STATION	OUTSTATION
NOTE: This brief use of transferred key is authorized and is not a reportable COMSEC incident.	**NOTE**: This brief use of transferred key is authorized and is not a reportable COMSEC incident.
18. If all receiving OSs do not respond, turn KY-57/58/67 KEY FILL switch to fill position 6, advise stragglers that steps 11 thru 17 will be repeated, and direct them to acknowledge.	Stragglers respond in polling order.
19. Repeat steps 10 thru 16 for stragglers. **NOTE**: If there are no stragglers omit steps 18 and 19.	Stragglers respond as directed by NCS.
20. Call net, announce that OTAT of key (tag) is complete, advise if additional keys are to be transferred, and direct OSs to acknowledge.	Respond in polling order.
21. If additional keys are to be transferred, repeat steps 4 - 20. **NOTE**: If no further keys are to be transferred, omit step 21.	React as directed by NCS.
22. When all keys are transferred direct receiving OSs to acknowledge and to turn KY-57/58/67 KEYFILL switch to effective TEK.	Acknowledge in polling order, and then turn KY-57/58/67 KEY FILL switch to effective TEK.
23. Turn KY-57/58/67 KEY FILL switch to effective TEK.	Wait.
24. Poll net, authorize OSs to resume normal net operation, and direct OSs to acknowledge.	Acknowledge in polling order, and resume communications.
25. Turn "OFF" all KYX-15 ADDRESS SELECT toggle switches.	Turn "OFF" all KYX-15 ADDRESS SELECT toggle switches.
26. Turn KYX-15 MODE switch to "OFF/CK".	Turn KYX-15 MODE switch to "OFF/CK".
27. Disconnect KYX-15 from KY-57/58/67.	Disconnect KYX-15 from KY-57/58/67.
28. Log OTAT activity.	Log OTAT activity.

THIS PAGE IS INTENTIONALLY BLANK

ANNEX F

(U) KYV-5, KY-99, KY-99A, AND KY-100 OTAD PROCEDURES

1. (U) **INTRODUCTION** - The cryptographically compatible KYV-5, KY-99/99A, and KY-100 Advanced Narrowband Digital Voice Terminal (ANDVT) equipment are designed to secure voice point-to-point circuits and multi-station nets. ANDVT terminal configurations are identified below.

NOTE: (U//FOUO) The AN/CSZ-1A SUNBURST Processor is a portable tactical secure communications unit that is cryptographically compatible with ANDVT equipment, but that may not serve as an OTAR NCS. The CSZ-1A is capable of automatic rekeying (AK) OTAR, but not of manual rekeying (MK) OTAR or of OTAT.

a. (U) **TACTERM** - The ANDVT tactical terminal (TACTERM) is intended for airborne, shipboard, ground vehicular, and fixed-plant applications. It is comprised of the KYV-5 COMSEC Module and the CV-3591 Basic Terminal Unit. The Z-ANG/Z-ANH remote control unit permits operation in aircraft.

b. (U) **MINTERM** - The KY-99 and KY-99A miniature terminal (MINTERM) are light-weight, battery-powered terminals that are intended for half-duplex, man-pack applications.

NOTE: (U//FOUO) The principal functional differences between the KY-99 and KY-99A are that the latter does not have a lock/unlock function, but has a separate logic that is cryptographically compatible with the KY-57/58/67 (VINSON) cryptosystem. Separate keys must be used for ANDVT and VINSON applications.

c. (U//FOUO) **AIRTERM** - The KY-100 (AIRTERM) was developed for use in fixed and rotary wing aircraft and small watercraft where KYV-5s cannot be used. The AIRTERM has a two-chassis configuration consisting of a KY-100 main terminal that is mechanically similar to the KY-58 and a Z-AVH remote control unit that permits remote operation of the KY-100. The KY-100 incorporates all of the capabilities of the KY-99A, including a VINSON mode, and an emergency backup key (EBK) that allows a zeroized terminal to be used for voice privacy in COMSEC emergencies associated with law enforcement operations.

NOTE: (UFOUO) A crypto-ignition key (CIK) was designed into the KY-100 to declassify keyed but unmanned terminals; however, this function proved unreliable and has been disabled.

2. (U) **PURPOSE AND SCOPE** - This annex provides standard procedures to cold start ANDVT equipment, to generate key, and to accomplish OTAR and OTAT.

CAUTION: (U) Prior to cold starting ANDVT equipment or performing OTAR or OTAT procedures, ensure that any fill device to be used is functioning properly and has sufficient battery energy to complete the operation.

3. (U) **ANDVT COLD START**

a. (U//FOUO) **Using Start-up KEK or Common KEK** - To cold start an ANDVT secured net or circuit that is being established with start-up KEK or that uses common KEK held by all OSs, use the following steps:

NET CONTROL STATION	OUTSTATION
1. Prior to net activation, load designated segment of KEK or start-up KEK in ANDVT fill positions 1 and U.	Prior to net activation, load designated segment of KEK or start-up KEK in ANDVT fill positions 1 and U.
2. Update key in ANDVT fill position 1.	Update key in ANDVT fill position 1.
3.a. Set KV-5 DATA/VOICE switch to “NET” or “P-T-P”, as appropriate.	Set KYV-5 DATA/VOICE switch to “NET” or “P-T-P”, as appropriate.
3.b. Set KY-99/99A/100 FUNCTION switch to “CT”.	Set KYV-99/99A/100 FUNCTION switch to “CT”.
4. Set ANDVT KEY FILL switch to fill position 1.	Set ANDVT KEY FILL switch to fill position 1.
5. Poll net.	Respond in polling order.
6. After all OSs have responded, replace key in ANDVT fill position 1 via non-cooperative AK OTAR.	Wait.

NOTE: (U//FOUO) Failure to perform step 2. is a reportable COMSEC incident.

b. (U//FOUO) **Using Multiple KEKs -** To cold start an OTARing ANDVT secured net that uses multiple KEKs (either a unique KEK for each OS or a combination of OS-unique and common KEKs), the NCS and OS use the following steps:

NET CONTROL STATION	OUTSTATION
1. Prior to net activation, load designated segment of each KEK in KYX-15 fill positions 16 thru 2.	Take no action.
2. Load KEK of first OS to get new TEK in ANDVT fill positions 1 and U.	Prior to net activation, load designated segment of KEK in ANDVT fill positions 1 and U.
3. Update key in ANDVT fill position 1.	Update key in ANDVT fill position 1.
4.a. Set KYV-5 DATA/VOICE switch to “NET”.	Set KYV-5 DATA/VOICE switch to “NET”.
4.b. Set KY-99/99A/100 FUNCTION switch to “CT”.	Set KY-99/99A/100 FUNCTION switch to “CT”.

NET CONTROL STATION	OUTSTATION
5. Set ANDVT KEY FILL to fill position 1.	Set ANDVT KEY FILL to fill position 1.
6. Poll net.	Respond in polling order.
7. After all OSs have responded, replace key in ANDVT fill position 1 via non-cooperative OTAR.	Wait.

NOTE: (U//FOUO) Failure to perform step 3. is a reportable COMSEC incident.

4. (U//FOUO) **ANDVT KEY GENERATION** - To generate key with an ANDVT, uses the following steps:

1. Connect KYX-15 to ANDVT.
2. Turn "ON" ANDVT power switch. **NOTE**: To generate key, ANDVT must contain any valid key in X1 key fill position.
3. Set KYX-15 MODE switch to "VG".
4. Turn "ON" KYX-15 toggle switch for vacant fill position.
5. Press and release KYX-15 INITIATE button. **NOTE**: KYX-15 PARITY light flashes, and “pass” tone is audible in handset. KYV-5 XMIT CIPH light goes out briefly, and KYV-5 displays “CC”. KY-99/99A/100 displays “NCD VG”.
6. Record purpose or tag of generated key on KYX-15 writing surface corresponding to fill position in which it is stored.
7. Set KYX-15 MODE switch to "OFF/CK".
8. Press and release KYX-15 INITIATE button. **NOTE**: KYX-15 PARITY light blinks.
9. Turn "OFF" KYX-15 toggle switch.
10. Repeat steps 4 thru 9 as often as necessary to generate additional required keys.
11. Disconnect KYX-15 from ANDVT.

5. (U//FOUO) **ANDVT NON-COOPERATIVE AK OTAR** - This is the recommended means for replacing TEK on ANDVT secured nets and circuits. It may be accomplished either simultaneously, for all OSs that hold KEK in common, or sequentially, one OS or group of OSs at a time, depending on how KEK is allocated. Although the sequential method requires more net time, it is frequently used in small, high-speed nets, because it is less prone to error and because it allows the NCS to withhold new TEK from OSs that have been captured. To accomplish non-cooperative AK OTAR, the NCS performs the following steps:

NOTE: (U) This procedure is “non-cooperative”, since it requires no actions by OS operators (other than responding to NCS polls and calls). To support OTAR, an ANDVT net or circuit must be active, with all net OSs in secure communication with the NCS.

NOTE: (U) Between OTAR cycles, the NCS stores all KEKs in a KYX-15, but each OS stores its KEK in its ANDVT.

1. Connect KYX-15 containing new TEK and all OS KEKs to ANDVT.
2. Load TEK to be transferred into ANDVT fill position and record its number.
3. Set KYX-15 MODE switch to "AK".
4. Poll net, notify OSs to prepare for a non-cooperative AK OTAR, and direct them to refrain from transmitting until OTAR routine is complete.
5. Turn "ON" KYX-15 toggle switch of one OS KEK.
6. Turn "ON" KYX-15 toggle switch of TEK being transferred.
7. Press KYX-15 INITIATE button. **NOTE**: KYV-5 CT light goes out briefly, data preamble sidetone is audible in handset, and ALARM light flashes. **NOTE**: KY-99/99A/100 displays "TX AK", and transmit modem tone is audible in handset.
8. Turn "OFF" KYX-15 toggle switch for OS KEK.
9. Using new TEK, call receiving OS (or poll net, if simultaneous OTAR approach is being used).
10. If receiving OS (or any OSs) failed to respond, repeat steps 6 thru 9, using old TEK and each straggler's OS KEK. **CAUTION**: Before completing step 11, ensure that all OSs have received the new TEK.
11. Turn "OFF" KYX-15 toggle switch for new TEK.
12. Turn KYX-15 MODE switch to "VU".
13. Turn "ON" KYX-15 toggle switch for KEK of OS that received TEK (or the common net KEK, if used). **NOTE**: All other KYX-15 toggle switches must be "OFF".
14. Press and release KYX-15 INITIATE button. **NOTE**: KYX-15 PARITY light flashes. **NOTE**: KYV-5 XMIT CIPH goes out briefly, and KYV-5 displays "CC" for a few seconds. **NOTE**: KY-99/99A/100 displays "NCD VU", and "pass" tone is audible in handset.

16. Turn KYX-15 MODE switch to "OFF/CK".
17. If sequential OTAR method is used, repeat steps 6 thru 15, using a different OS KEK, until all OSs have received new TEK and all KEKs are updated. **NOTE**: If simultaneous OTAR method is used, omit this step.: If simultaneous OTAR method is used, omit this step.
18. Poll net and direct resumption of communications.
19. Turn KYX-15 MODE switch to "OFF/CK".
20. Disconnect KYX-15 from ANDVT.
21. Record time and date of OTAR cycle, location of new TEK in ANDVT, and changes in net composition, if any.

6. (U//FOUO) **ANDVT COOPERATIVE AK OTAR** - This procedure is the recommended means of passing non-extractable TEK to distant ANDVT equipment, for use at a later time or so that the receiving equipment may enter another cryptonet. To accomplish cooperative AK OTAR, use the following steps:

> **NOTE:** This procedure is “cooperative”, since it requires actions by each OS operator. It may be accomplished either sequentially or simultaneously, depending on how KEK is allocated in the net.

NET CONTROL STATION	OUTSTATION
1. Connect KYX-15 containing key to be transferred and all OS KEKs to ANDVT.	Communicate normally.
2. Turn "ON" KYX-15 toggle switch for key being transferred.	Communicate normally.
3. Turn "ON" KYX-15 toggle switch for net KEK (with simultaneous procedure) or one OS KEK (with sequential procedure).	Communicate normally.
4. Poll net, notify OSs to prepare for cooperative AK OTAR, advise OSs that will receive key of its purpose (advise tag if key is not future TEK for use on passing net), and direct OSs to refrain from transmitting until OTAR is complete.	Respond in polling order, and record purpose of key to be received.
5. Turn KYX-15 MODE switch to "AK".	Wait.
6. Direct OSs to set KYV-5 DATA/VOICE switch or KY-99/99A/100 FUNCTION switch to “RK” and to wait.	Set KYV-5 DATA/VOICE switch or KY-99/99A/100 FUNCTION switch to “RK” and wait. **NOTE**: KYV-5 XMT CIPH light goes out.

NET CONTROL STATION	OUTSTATION
7. Press KYX-15 INITIATE button. **NOTE:** KYX-15 PARITY light flashes. **NOTE**: KYV-5 XMIT CIPH light goes out briefly and comes back on, and AK preamble sidetone is audible in handset. **NOTE**: KY-99/99A/100 displays "TK AK", and transmit modem signal is audible in handset.	Wait. **NOTE**: If successful transfer occurred, KYV-5 displays constant "CC". **NOTE**: If successful transfer occurred, KY-99/99A/100 displays "LOAD" (with "1" flashing).
8.a. Wait.	KYV-5 OS turn KEY FILL switch to vacant fill position and push KYV-5 INITIATE switch. **NOTE**: KYV-5 loads received key into selected fill position and displays "01".
8.b. Wait.	KY-99/99A/100 OS press button to select vacant KEY button to select vacant KEY FILL position, and press KY-99/99A/100 INIT button to enter key. **NOTE**: At first push, KY-99 99A/100 displays flashing "LOAD #" (# is selected fill position). At second push, KY-99/99A/100 stores key and displays "KEY #" briefly. "Pass" tone is audible in handset.
9. Poll net (if simultaneous OTAR procedure used) or call OS (if sequential procedure used) and direct OS(s) to turn KYV-5 DATA/VOICE switch to “NET” or KY-99/99A/100 FUNCTION switch to “CT” and to respond in polling order. **CAUTION**: Before completing step 10, ensure that all OSs that should respond do so.	Turn KYV-5 DATA/VOICE switch to “NET” or KY-99/99A/100 FUNCTION switch to “CT” and respond, in polling order, to confirm successful key transfer.
10. Turn "OFF" KYX-15 toggle switch for transmitted key.	Wait.
11. Turn KYX-15 MODE switch to “VU”.	Wait.

NET CONTROL STATION	OUTSTATION
12. Turn "ON" KYX-15 toggle switch for net KEK or OSs that received key. **NOTE**: All other KYX-15 toggle switches must be "OFF".	Wait.
13. Press KYX-15 INITIATE button **NOTE**: KYX-15 PARITY light flashes and a "pass" tone is audible in handset. KYV-5 XMIT CIPH light goes off briefly. **NOTE**: KYV-5 XMIT CIPH light goes off briefly. **NOTE**: KY-99/99A/100 displays "NCD VU".	Wait.
14. Turn "OFF" KYX-15 toggle switches.	Wait.
15. If sequential OTAR procedure is used, repeat steps 6 thru 17, using KEK of called OS, until key is transferred to all OSs. **NOTE**: If net KEK is used, omit this step.	Perform actions as steps 6 thru 17 require.
16. If other keys are to be transferred, repeat steps 5 thru 15 until all keys have been transferred.	Perform actions as steps 5 thru 15 require.
17. Call net and direct resumption of communications.	Acknowledge in polling order and resume communications.
18. If transferred key is future net TEK, load it into desired ANDVT fill position, and record its location. **NOTE**: If transferred key is not future TEK, omit this step.	Communicate normally.
19. Turn KYX-15 MODE switch to "OFF/CK".	Communicate normally.
20. Disconnect KYX-15 from ANDVT	Communicate normally.
21. Record time and date of OTAR activity, including tags of keys transferred that are not future TEKs for use on transmitting net or circuit.	

7. (U//FOUO) **ANDVT OTAT** - This procedure is used to transfer key that will be extracted at the OSs and used to key another COMSEC equipment, either an ANDVT that is used on another net or circuit or, in COMSEC emergencies, any COMSEC equipment capable of using 128-bit key. To accomplish ANDVT OTAT, use the following steps:

NOTE: (U//FOUO) ANDVT OTAT must be performed sequentially. It is “cooperative”, since it requires actions by OS operators. If a common KEK is used, all net OSs have the potential to receive the transferred key, but the NCS may specify those that are required to do so.

NOTE: (U//FOUO) Except during COMSEC emergencies, KEKs may not be transmitted electrically.

NET CONTROL STATION	OUTSTATION
1. Connect KYX-15 containing key to be transferred to ANDVT.	Communicate normally.
2. Turn "ON" KYX-15 toggle switch for key to be transferred.	Communicate normally.
3. Turn "ON" KYX-15 toggle switch for net KEK or unique KEK for one OS that will receive key.	Communicate normally.
3. Turn "ON" KYX-15 toggle switch for net KEK or unique KEK for one OS that will receive key.	Communicate normally.
4. Poll net, alert OSs that OTAT activity is about to take place, and direct them to refrain from transmitting until the routine is complete.	Respond in polling order.
5. Call net or receiving OS and advise "tag" of key to be transmitted.	Respond (in polling order, if net KEK is used), and record "tag" of key to be received.
6. Turn KYX-15 MODE switch to "AK".	Wait.
7. Direct receiving OS(s) to connect KYK-13 or KYX-15 to ANDVT, to select vacant KYX-15/ KYK-13 fill position, and to record its number.	Connect KYK-13 or KYX-15 to ANDVT, turn "ON" vacant KYX-15 or KYK-13 toggle switch, and record its number.
8. Direct receiving OS(s) using KYX-15 to turn its MODE switch to "LD".	OSs using KYX-15 turn MODE switch to "LD".
9. Direct receiving OS(s) to turn KYV-5 DATA/ VOICE switch or KY-99/99A/100 FUNCTION switch to “RK” and to press KYX-15/KYK-13 INITIATE button.	Turn KYV-5 data/voice switch or KY-99/ 99A/100 FUNCTION switch to “RK” and press KYX-15/KYK-13 INITIATE button.

NET CONTROL STATION	OUTSTATION
10. Press KYX-15 INITIATE button. **NOTE**: KYX-15 PARITY light flashes. **NOTE**: KYV-5 XMIT CIPH light goes out briefly, and AK preamble sidetone is audible in handset. **NOTE**: KY-99/99A/100 displays: KY-99/99A/100 displays audible in handset.	Wait. **NOTE**: KYK-13/KYX-15 PARITY light flashes. **NOTE**: KYV-5 displays "EO" briefly then "CC". **NOTE**: KY-99/99A/100 displays "TK AK" and transmit modem signal is audible in handset.
11. Poll net (if common KEK used) or call OS (if multiple KEKs are used) and direct OS(s) to set KYV-5 DATA/VOICE switch to “NET” or “P-T-P” (as appropriate) or to turn KY-99/99A/100 FUNCTION switch to “CT”, and verify that key was received. **CAUTION**: Ensure that receiving OS (or all addressed OSs, if common KEK used) verify receipt of key, before completing step 12.	Turn KYV-5 DATA/VOICE switch to “NET” or “P-T-P” (as appropriate) or KY-99/99A/100 FUNCTION switch to “CT”, and to respond in polling order, if key was received
12. Turn "OFF" all KYX-15 toggle switches.	Wait.
13. Turn KYX-15 MODE switch to "VU".	Wait.
14. Turn "ON" KYX-15 toggle switch of net KEK or KEK of OS that received key. 15. Press KYX-15 INITIATE button. **NOTE**: KYX-15 PARITY light flashes **NOTE**: KYV-5 XMIT CIPH light goes out briefly, KYV-5 displays "CC", out briefly, KYV-5 displays "CC", and "pass" tone is audible in handset. **NOTE**: KY-99/99A/100 displays "NCD VU" and "pass" tone is audible in handset.	Wait. Wait.
16. Turn "OFF" KYX-15 toggle switch.	Wait.
17. If multiple KEKs are used, repeat steps 6 thru 16, using KEK of each other OS to receive key, until all desired OSs verify key receipt.	Comply as required by steps 6 thru 16.

NET CONTROL STATION	OUTSTATION
18. If additional keys are to be transferred, repeat steps 6 thru 17.	Comply as required by steps 6
19. Record date and time, tag, recipient(s) or all OTATed key.	Record date and time of each key received.
20. Poll net and direct resumption of normal communications.	Respond in polling order and resume normal communications.
21. Turn KYX-15 MODE switch to "OFF/CK".	Communicate normally.
22. Disconnect KYX-15 from ANDVT.	Communicate normally.

ANNEX G

(U) KY-68 OTAD PROCEDURES

1. (U) **INTRODUCTION** - The KY-68 Digital Secure Voice Terminal (and its fixed-plant functionally equivalent, the KY-78) are capable of both OTAR and OTAT, when they are installed in connection with TRI-TAC and MSE systems and in sole-user applications.

> **NOTE**: (U//FOUO) In the sole-user mode of operation, two KY-68s are connected back-to-back, with no intervening switching equipment. Both keyboards are disabled, and signalling is accomplished automatically. When the calling terminal goes off-hook, the receiving terminal rings, and conversation can begin when the receiving terminal goes off-hook. The sole-user mode does not permit plain text operation.

2. (U) **PURPOSE AND SCOPE** - This annex provides standard procedures for accomplishing OTAR on sole-user KY-68 circuits and OTAT on sole-user and TRI-TAC/MSE circuits secured by the KY-68.

> **CAUTION**: (U) Prior to performing OTAR or OTAT on KY-68 circuits, ensure that any fill device to be used is functioning properly and has sufficient battery energy to complete the operation.

3. (U//FOUO) **SOLE-USER KY-68 OTAR** - This procedure is used to remotely rekey sole-user KY-68 terminals. KY-68s can also be rekeyed by the operator at the associated TRI-TAC or MSE switch, but that process is beyond the scope of this manual. To accomplish sole-user KY-68 OTAR, the calling terminal operator uses the following steps, after the answering terminal operator answers the call:

> **NOTE**: (U) Sole-user KY-68 OTAR requires that both KY-68s hold the same KEK and TEK.

1. Load KEK into higher numbered KYX-15 fill position.
2. Load new TEK into lower numbered KYX-15 fill position.
3. Connect KYX-15 to KY-68 with fill cable.
4. Call receiving terminal in secure mode and inform receiving operator that OTAR will occur.
5. Set KYX-15 MODE switch to "AK".
6. Turn "ON" KYX-15 toggle switch for KEK and TEK. **NOTE**: All other KYX-15 toggle switches must be "OFF".
7. Push and release KYX-15 INITIATE button. **NOTE**: The OS KY-68 now holds the new TEK, but the NCS KY-68 does not. To supply TEK for future secure calls, the NCS operator must load the new TEK into his KY-68 from the KYX-15.
8. Turn KYX-15 MODE switch to "OFF/CK".

9. Disconnect KYX-15 from KY-68.

4. (U//FOUO **KY-68 OTAT** - To transfer key from one KYX-15 to another via TRI-TAC/MSE or sole-user KY-68s, use the following steps:

NOTE: (U) KY-68 OTAR is “cooperative”, because it requires actions by the receiving terminal operator.

CALLING TERMINAL	ANSWERING TERMINAL
1. Load appropriate TRI-TAC, MSE or sole-user KEK in vacant KYX-15 fill position.	Take no action.
2. Load keys to be transferred in vacant KYX-15 fill positions.	Take no action.
3. Call receiving KY-68, advise number of keys to be transferred and their tags, and direct receiving KY-68 to verify that KEK is held.	Respond, load KEK in vacant KYX-15 fill positions, and record key tags in sequence given.
4. Connect KYX-15 to KY-68.	Connect KYX-15 to KY-68.
5. Wait.	Turn "ON" KYX-15 toggle switch for KEK. **NOTE**: All other KYX-15 toggle switches must be "OFF".
6. Wait.	Turn KYX-15 MODE switch to "LD".
7. Wait.	Move KY-68 VAR STOR switch to "LOAD" and release. **NOTE**: Two PARITY tones are audible.
8. Turn "ON" KYX-15 toggle switch for first or next key to be transferred. **NOTE**: Other KYX-15 toggle switches must be "OFF".	Select KYX-15 fill position for key to be received, and turn "ON" its toggle switch. **NOTE**: Other KYX-15 toggle switches must be "OFF".
9. Turn KYX-15 MODE switch to "LD".	Turn KYX-15 MODE switch to "RV".
10. Move KY-68 VAR STOR switch to "LOAD". **NOTE**: Two PARITY tones are audible.	Wait.
11. Turn KYX-15 toggle switch for key to be transferred.	Wait.
12. Turn "ON" KYX-15 toggle switch for UIRV or KEK.	Wait.

CALLING TERMINAL	ANSWERING TERMINAL
13. Turn KYX-15 MODE switch to "MK". **NOTE**: Circuit loses sync, and static is audible at NCS.	Push and release KYX-15 MODE INITIATE button.
14. Wait for sync loss, then push and release KYX-15 INITIATE button. **NOTE**: KYX-15 PARITY light flashes and circuit syncs.	Wait. **NOTE**: KYX-15 PARITY light flashes and circuit syncs.
15. Move KYX-15 MODE SELECT switch to "OFF/CK".	Turn KYX-15 MODE switch to "OFF/CK".
16. Wait.	Move KY-68 VAR STOR switch to "LOAD" and release. **NOTE**: KYX-15 PARITY light flashes.
17. Repeat steps 5 thru 16 for each additional key to be transferred.	Repeat steps 5 thru 16 for each additional key to be transferred.
18. Disconnect KYX-15 from KY-68.	Disconnect KYX-15 from KY-68.
19. Return KY-68 to "on-hook" position.	Return KY-68 to "on-hook" position.

THIS PAGE IS INTENTIONALLY BLANK

ANNEX H

(U) KW-46 OTAD PROCEDURES

1. (U) **PURPOSE** - This annex provides standardized instructions for accomplishing OTAT and CV OTAR on KW-46 secured broadcasts.

2. (U//FOUO) **LOADING KEY** - Broadcast Control Station (BCS), BCS on-air monitor, and Receiving Stations (RS) must load the same CV into KW-46 fill position CV-1 and the same KEK into fill position CV-2, using following steps:

NOTE: (U) Procedures for loading CVs and KEKs are stated in terms of the KOI-18; however, key may also be loaded using the KYK-13, the KYX-15, and the AN/CYZ-10. All numbered steps and associated notes and cautions are "UNCLASSIFIED//FOR OFFICIAL USE ONLY".

CAUTION: (U) Prior to loading key into a KW-46 or performing OTAR or OTAT procedures, ensure that any fill device to be used is functioning properly and has sufficient battery energy to complete the operation.

1. Connect KOI-18 to KW-46 with fill cable.
2. On KW-46 depress "21" (for CV) or "22" (for KEK), "ENTER", "VERIFY", and "EXECUTE". **NOTE**: KW-46 BUSY and KEY I/O lights come on. **NOTE**: BCS, BCS on-air monitor, and RS must have KEK in same KW-46 fill position. If BCS directs that KEK be loaded into a fill position other than 22, load commands change accordingly, for example, load command 23 for KEK-
3. Pull key tape through KOI-18. **NOTE**: KW-46 BUSY and KEY I/O lights go out.

3. (U) **OTAT/OTAR PROCEDURES** - KW-46 OTAT/OTAR procedures are stated below.

NOTE: (U//FOUO) Because most of the procedural steps for accomplishing OTAT and OTAR are similar, they are presented in a single list. OTAT uses steps 1 - 24 and 29 thru 33, and OTAR uses steps 1 - 16 and 25 - 33. BCS on-air monitor follows procedure for RS. All numbered steps and associated notes and cautions are UNCLASSIFIED//FOR OFFICIAL USE ONLY"

BROADCAST CONTROL STATION
CAUTION: BCS KWT-46 must be set to red mark input (no traffic).
1. Press "53". **NOTE**: Display reads "LINK CM".

2. Press “000001”, “ENTER”, “VERIFY”, “VERIFY”, and “EXECUTE”. **NOTE**: LINK light goes out. (RS LINK light also goes out.)
3. Press “51”. **NOTE**: Display reads “ACC ID”, and DATA light comes on.
4. Enter 4-digit octal number assigned as key ID. **CAUTION**: 4-digit key ID must be identical to that assigned in key transfer notice message and cannot be all zeros or ones.
5. Press “ENTER” and “VERIFY”. **NOTE**: Display reads “ACC ID”.
6. Press "VERIFY". **NOTE**: Display reads 4-digit key ID.
7. Press “EXECUTE”. **NOTE**: Steps 8.a - 8.g cover loading key to be transferred from KYK-13; steps 9.a - 9.g cover loading such key from KYX-15; and steps 10.a - 10.e. cover loading it from KOI-18. See Annex J for corresponding AN/CYZ-10 procedures.
8.a. Connect KYK-13 to KWT-46 (with fill cable, if desired).
8.b. Turn KYK-13 ADDRESS SELECT switch to fill position of key to be passed.
8.c. Turn "ON" KYK-13 MODE switch.
8.d. On KWT-46 press "35". **NOTE**: KWT-46 display reads "ACSV RK".
8.e. On KWT-46 press "ENTER", "VERIFY", and "EXECUTE". **NOTE**: KYK-13 PARITY light and KWT-46 BUSY and KEY I/O lights blink.
8.f. Turn “OFF” KYK-13 MODE switch.
8.g. Disconnect KYK-13 from KWT-46.
9.a. Connect KYX-15 to KWT-46 with fill cable.
9.b. Turn “ON” KYX-15 toggle switch for key to be transferred.
9.c. Turn KYX-15 MODE switch to “LD”.

9.d. On KWT-46 press “35”. **NOTE**: KWT-46 display reads “ACSV RK”.
9.e. On KWT-46 press “ENTER”, “VERIFY”, and “EXECUTE”. **NOTE**: KYX-15 PARITY light and KWT-46 BUSY and KEY I/O lights blink.
9.g. Disconnect KYX-15 from KWT-46.
9.f. Turn KYX-15 MODE switch to "OFF/CK".
10.a. Connect KOI-18 to KWT-46 with fill cable.
10.b. On KWT-46 press "35". **NOTE**: KWT-46 display reads "ACSV RK".
10.c. On KWT-46 press "ENTER", "VERIFY", and "EXECUTE". **NOTE**: KWT-46 BUSY and KEY I/O lights come on.
10.d. Pull tape thru KOI-18. **NOTE**: KWT-46 BUSY and KEY I/O lights go off.
10.e Disconnect KOI-18 from KWT-46.

BROADCAST CONTROL STATION	RECEIVING STATION
11. On KWT-46 press "53". **NOTE**: KWT-46 display reads "LINK CM" and its DATA light comes on.	**NOTE**: KWR-46 LINK light comes on for approximately 50 seconds during transfer and goes out on completion. KWR-46 UVRQ/REKEY light comes on, and KWR-46 becomes subject to two-person integrity (TPI) rules unless received key is not intended for use by receiving unit. In that situation, a single operator may zeroize KWR-46 UVRQ fill position if done immediately.
12. On KWT-46 press "001150" **NOTE**: KWT-46 DATA light goes out.	Wait.
13. On KWT-46 press “ENTER”, “VERIFY”, “VERIFY”, and “EXECUTE”.	Wait.
14. Repeat steps 3. - 13. for each additional key to be transmitted.	Repeat steps 3. - 13. for each additional key to be transmitted.

RECEIVING STATION
15. On KWR-46 press “54”. **NOTE:** KWR-46 display reads “VARP”.
16. On KWR-46 press “ENTER”. **NOTE:** KWR-46 display reads 4-digit octal number BCS assigned in key transfer notice message; see step 4. **NOTE:** If OTAR, omit steps 17 - 24 and proceed with step 25.
17. Connect KYK-13/KYX-15 to KWR-46 fill port.
RECEIVING STATION
18. On KWR-46 press “59”. **NOTE:** KWR-46 display reads “ORKV”.
19. On KWR-46 press “ENTER”, “VERIFY”, and “EXECUTE”. **NOTE:** KWR-46 BUSY and KEY I/O lights come on. **NOTE:** Use steps 20.a & 20.b for KYK-13 key extraction or steps 21.a & 21.b for KYX-15 key extraction. See Annex J for AN/CYZ-10 procedures.
20.a Turn KYK-13 ADDRESS SELECT toggle to location chosen to receive OTAT key.
20.b Turn “ON” KYK-13 MODE switch.
21.a Turn “ON” KYX-15 toggle switch chosen to receive OTAT key.
21.b Turn “ON” KYX-15 MODE switch.
22. Press KYK-13 OR KYX-15 INITIATE button. **NOTE:** KYK-13/KYX-15 PARITY light blinks and KWR-46 BUSY, and KEY I/O light goes out. **CAUTION:** As long as KWR-46 UVRQ/REKEY light is on, KWR-46 is subject to TPI rules. Key remains available until a positive action is taken to zeroize it. This is done by the “85” - RSET RK”
23. Turn “OFF” KYK-13/KYX-15 MODE switch.
24. Disconnect KYK-13/KYX-15 from KWR-46.
25. On KWR-46 press “7”. **NOTE:** KWR-46 display reads “LRKV”. **NOTE:** To load OTAR CV in a CV fill position other than CV-1 or CV-2 use steps 25 - 27.

26. On KWR-46 press “3” (for CV-3), “ENTER”, “VERIFY”, and “EXECUTE’. **CAUTION:** As long as UVRQ light is on, KWR-46 is subject to TPI rules.
27. On KWR-46 press “85”. **NOTE:** KWR-46 display reads “RSET RK”.
28. On KWR-46 press “ENTER”, “VERIFY”, and “EXECUTE’. **NOTE:** KWR-46 UVRQ/REKEY light goes out and KWR-46 is no longer subject to TPI rules. **NOTE:** Repeat steps 3-37 for each additional key to be passed via OTAT or OTAR. BCS must allow at least one minute for RSs to extract or park each transmitted key. **NOTE:** After last key is passed, wait at least 2 minutes before going back to traffic.

BROADCAST CONTROL STATION	RECEIVING STATION
29. On KWR-46 press “53”. **NOTE:** KWT-46 display reads “LINK CM”.	Wait.
30. On KWT-46 press “001000”, “ENTER”, “VERIFY”, “VERIFY”, and “EXECUTE”. **NOTE:** KWR-46 on-line monitor LINK light comes on, and UVRQ/REKEY light blinks off briefly and then comes back on.	Wait. **NOTE:** KWR-46 LINK light comes on.
31. On KWT-46 remove red mark and resume traffic	Wait. **NOTE:** Traffic flow resumes.
32. On KWR-46 (on-air monitor) press “85”. **NOTE:** KWR-46 display reads “RSET RK”.	Take no action.
33. On KWR-46 on-air monitor press “ENTER”, “VERIFY”, and “EXECUTE”. **NOTE:** KWR-46 UVRQ/REKEY light goes out.	Take no action.

THIS PAGE IS INTENTIONALLY BLANK

ANNEX I

(U) OTAR AND OTAT USING AN/CYZ-10

1. (U) **INTRODUCTION**

a. (U//FOUO) **Capabilities -** The AN/CYZ-10 data transfer device is capable of emulating the KYX-15 net control device, the KYK-13 electronic transfer device, and the KOI-18 tape reader (without being able to read punched tape) in support of OTAR and OTAT. It is also capable of introducing unencrypted (i.e., RED) key or encrypted (i.e., BLACK) key into a STU-III, STU-IIIA, STE, or Allied STU-IIB data port and extracting it, in the same form, at a distant STU-III, STU-IIIA, STU-IIB, or STE terminal.

NOTE: (U) Although the procedures are identical for transferring RED and BLACK key from one DTD to another via a secure telephone, this document only applies to RED key transfers.

b. (U) **Purpose** - This annex states abbreviated procedures for accomplishing processes that affect OTAR and OTAT on nets/circuits that are secured by the KG-84A/C, KY-57/58/67, and KYV-5 and KY-99/99A/100, and OTAT on KW-46 secured broadcasts, KY-68 secured voice circuits, and STU-III/IIIA/IIB/STE secured telephone circuits.

NOTE: (U//FOUO) The procedures presented in this annex are based on NSA developed "F4.09" software for the DTD. Procedural changes will be made when "Common Tier 3" software is implemented.

2. (U//FOUO **EMULATING COMMON FILL DEVICES** - To configure a CYZ-10 to emulate a KYX-15 or KYK-13, use the following steps:

1. From main menu, select "Appl" and "Fill".
2. From fill main menu, select "Utility", "Setup", "Protocol", "Cfd" and either "13" or "15", as appropriate.

3. (U//FOUO) **LOADING DTD FROM KOI-18** - To load a DTD from a KOI-18, use the following steps:

1. Set up DTD to emulate KOI-18, and select Abort.
2. From DTD fill main menu, select "Recv".
3. Connect DTD to KOI-18.
4. Press RCV key on DTD.
5. Pull key tape through KOI-18.
6. Enter key tag as prompted by DTD.

4. (U) **LOADING DTD FROM ANOTHER DTD**

a. (U//FOUO) **Data Standard** - Setup both DTDs to “DS-101”, using “Utility”, “Setup”, and “Protocol” from fill main menu.

b. (U//FOUO) **Sending DTD** performs following steps:

1. From fill main menu, select “Xmit” and “Issue”.
2. Use P UP and P DN keys to scroll thru key data base and ENTR key to select key(s) to be transferred.
3. Select “Send”, when finished selecting key(s), and select “Direct”.
4. Connect sending and receiving DTDs.
5. Press SEND key.

c. (U//FOUO) **Receiving DTD** performs following steps:

1. From fill main menu, select “Recv”.
2. Press RCV key. **NOTE**: Key tag data will also be transferred to receiving DTD.
3. Disconnect sending and receiving DTDs.

5. (U//FOUO) **LOADING COMSEC EQUIPMENT FROM DTD** - To load an OTAR capable COMSEC equipment from a DTD, use the following steps:

1. Set up DTD to emulate KYX-15 or KYK-13.
2. From DTD fill main menu, select “Xmit”.
3. Use DTD P UP and P DN keys to scroll thru key data base and ENTR key to select key(s) to be transferred.
4. Select “Send”, when finished selecting key(s).
5. Connect DTD to COMSEC equipment.
6. Press DTD CLR key.
7. Press DTD SEND key.
8. Press "initiate" on COMSEC equipment.
9. Disconnect DTD from COMSEC equipment.

6. (U//FOUO) **PERFORMING MK OTAR** - When using a DTD in lieu of a KYX-15 to accomplish MK OTAR on a KG-84A/C or ANDVT secured point-to-point circuit (or to recover from KEK updating error on a ANDVT secured circuit, the NCS must perform the appropriate COMSEC equipment steps and the following steps with the DTD:

1. Set up DTD to emulate KYX-15.
2. From fill main menu, select “Net” and “Mk”.
3. Use DTD P UP and P DN keys to scroll thru key data base and ENTR key to select keys to be transferred.
4. Connect DTD to COMSEC equipment.
5. Press SEND key.
6. Disconnect DTD to COMSEC equipment.

7. (U//FOUO) **PERFORMING AK OTAR** - To accomplish AK OTAR on a KG-84A/C, KIV-7/7HS. KY-57/58/67, RT-1523/A, or KYV-5/KY-99/99A/100 secured multi-station net using a DTD in lieu of a KYX-15, the NCS performs the appropriate COMSEC equipment steps and the following steps involving the DTD:

1. Set up DTD to emulate KYX-15.
2. From fill main menu, select “Net” then “Ak”.
3. Press CLR key, and use DTD P UP and P DN keys to scroll thru KEK(s) to be used, and ENTR key to select KEK(s).
4. Press SEND when finished selecting KEKs.
5. Press CLR key, and use ENTR key to select TEK to be transferred.
6. Select “Send”.
7. Connect DTD to COMSEC equipment.
8. Press SEND key.
9. Disconnect DTD from COMSEC equipment.

8. (U//FOUO) **PERFORMING OTAT** - To accomplish OTAT on a KG-84A/C, KY-57/58/67, or ANDVT secured net or circuit using an DTD in lieu of a KYX-15, the DTDs at both the NCS and OS(s) must be set up to emulate KYX-15s.

a. (U//FOUO) **NCS** performs appropriate COMSEC equipment steps and following DTD steps:

1. From fill main menu, select “Net” then “Mk” or Ak”, as appropriate.
2. Use DTD P UP and P DN keys to scroll thru key data base and ENTR key to select key to be transferred.
3. Connect DTD to COMSEC equipment.
4. Press SEND key.
5. After selected key has been transferred, repeat steps 2 thru 4 for each additional key to be transferred.
6. After all keys have been transferred, disconnect DTD from COMSEC equipment.

b. (U//FOUO) **OSs** performs appropriate COMSEC equipment steps and following steps involving the DTD:

1. From fill main menu, select “Net” then “Ak”.
2. Connect DTD to COMSEC equipment.
3. Press RCV key.
4. When OTAT transmissions are completed, disconnect DTD from COMSEC equipment.

9. (U) **TRANSFERRING KEY AND TAG FROM ONE DTD TO ANOTHER VIA STU-III/ STU-IIIA/STU-IIB/STE TELEPHONE CIRCUITS**

NOTE: (U//FOUO) To transfer a RED key of any classification from one DTD to another using the data ports of attached STU-III, STU-IIIA, STU-IIB, or STE equipment, both secure telephones must be configured the same, with one of the following rates and modes: 2400 baud asynchronous, 4800 or 9600 baud synchronous. When both ends use STEs over Integrated Services Digital Network circuits, the STEs can be set up to 64,000 baud in synchronous mode. Additionally, the DTDs at the receiving and sending locations must be set for the "STU" protocol. If excessive transmission delays inhibit the DTDs from completing the key exchange, change both DTDs Time Out to the "Slow" option, to allow the DTDs more time to negotiate the exchange.

a. (U//FOUO) **Sending Operator** performs following steps:

1. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE. **NOTE**: A special connector cable (NSN 5810-O1-391-4212), that is not furnished with the DTD, is required to connect the DTD to the STU-III/STU-IIIA/STU-IIB/STE data port. These items may be ordered from USACCSLA Ft. Huachuca, AZ, Code: SELCL-IA, POC: Mr. Riensche, DSN: 870-8335, COML: (520) 538-8335.
2. Call intended receiver using STU-III/STU-IIIA/STU-IIB/STE secure voice mode and inform operator that tagged COMSEC key is to be transferred.
3. Verify with receiving operator that his DTD is set to “RS-232” mode and is connected to STU-III/STU-IIIA/STU-IIB/STE in use. **NOTE:** If not, from the fill main menu, select “Utility”, “Setup”, “Protocol”, and “Stu”.
4. Shift STU-III/STU-IIIA/STU-IIB/STE to secure data mode.
5. From DTD fill main menu, select “Xmit” and “Issue”.
6. Use ENTR and P DN keys to select keys to be transferred.
7. Press “SEND” when finished selecting keys.
8. Press DTD SEND key.
9. When all tagged keys have been transmitted, disconnect DTD from STU-III/STU-IIIA/ STU-IIB/STE.
10. Return STU-III/STU-IIIA/STU-IIB/STE to secure voice mode.

b. **Receiving Operato**r performs following steps:

1. Respond to sending operator's call and verify that DTD is attached to STU-III/STU-IIIA/ STU-IIB/STE being used. **NOTE**: See NOTE following paragraph 8.a., step 1regarding the special connector cable.
2. Verify that DTD is in “RS-232” protocol mode. **NOTE**: If not, from DTD fill main menu, select “Utility”, “Setup”, “Protocol”, and “Stu”.
3. From fill main menu, select “Recv”.
4. Press either DTD ENTR key or RCV key.
5. When all tagged keys have been received, disconnect DTD from STU-III/STU-IIIA/ STU-IIB/STE.

6. Return STU-III/STU-IIIA/STU-IIB/STE to secure voice mode and verify to sender that key was received.

10. (U) **TRANSFERRING JOINT TACTICAL INFORMATION DISTRIBUTION SYSTEM (JTIDS) KEY AND TAG FROM ONE DTD TO ANOTHER VIA STU-III/STU-IIIA/STU-IIB/ STE TELEPHONE CIRCUITS USING THE "FILL" THREAD OF JFILL USER APPLICATION SOFTWARE (UAS)**

NOTE: (U//FOUO) The DTD Joint fill (JFILL) routine has two branches or threads, i.e., the "FILL" thread and the "JTIDS" thread. DTD common tier three (CT3) UAS may also be used to transfer JTIDS key and data.

NOTE: (U//FOUO) To transfer a RED JTIDS key from one DTD to another using the data ports of attached STU-III, STU-IIIA, STU-IIB, or STE equipment, both secure telephones must be configured the same, with one of the following rates and modes: 2400 baud asynchronous, 4800 or 9600 baud synchronous. When both ends use STEs over Integrated Services Digital Network circuits, the STEs can be set up to 64,000 baud in the synchronous mode.

a. (U//FOUO) **Sending Operator** performs following steps:

1. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE, using connector cable identified in NOTE following paragraph 9.a., step 1.
2. Call intended receiver using STU-III/STU-IIIA/STU-IIB/STE secure voice mode and inform operator that tagged JTIDS key is to be transferred via JFILL (JTIDS) - JFILL (JTIDS) routine.
3. On DTD press "U" or select "Util" and press ENTR.
4. On DTD press "S" or select "Setup" and press ENTR.
5. On DTD press "P" or select "Protocol" and press ENTR.
6. On DTD press "R" or select "RS232" and press ENTR.
7. On DTD press "S" or select "Stu" and press ENTR.
8. On DTD press "X" or select "Xmit" and press ENTR.
9. On DTD press "S" and ENTR or press "A" to select all keys to select keys to transmit. **NOTE:** If "A" is selected, skip to step 12.
10. On DTD use P UP, P DN and ENTR to select keys to transmit.
11. On DTD press "Q" or select "Quit" and press ENTR to end key selection process.
12. On DTD observe "Connect to Station..." message.
13. On DTD press "SEND".

14. On DTD observe “STU-III” Connection Complete” message.
15. On DTD press “CLR”.
16. On DTD observe “Attempting to Connect” message and various other transfer messages.
17. When transfer is complete, disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

b. (U//FOUO) **Receiving Operator** performs following steps:

1. On STU-III/STU-IIIA/STU-IIB/STE acknowledge readiness to receive RED JTIDS key(s) using JFILL (JTIDS) - JFILL (JTIDS) routine.
2. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE.
3. On DTD press “U” or select “Util” and press ENTR.
4. On DTD press “S” or select “Setup” and press ENTR.
5. On DTD press “P” or select “Protocol” and press ENTR.
6. On DTD press “R” or select “RS232” and press ENTR.
7. On DTD press “S” or select “Stu” and press ENTR.
8. On DTD press “R” or select “Recv” and press ENTR.
9. On DTD observe “Connect to Station...” message.
10. On DTD press “Rcv”.
11. On DTD observe “STU-III Connection Complete” message.
12. On DTD press “CLR”.
13. On DTD observe “Attempting to Connect” message.
14. On STU-III/STU-IIIA/STU-IIB/STE press SECURE DATA button.
15. On DTD observe various transfer messages.
16. On STU-III/STU-IIIA/STU-IIB/STE when transfer is complete press SECURE VOICE button.
17. On STU-III/STU-IIIA/STU-IIB/STE acknowledge receipt of transferred keys.
18. Disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

NOTE: (U//FOUO) Key transfer is complete when Retransmit menu is displayed on transmitting DTD and “Connect to Station” is again displayed on receiving DTD.

NOTE: (U) Sending and receiving operators must record key transfers as required by their respective Services.

11. (U) **TRANSFERRING JTIDS KEY AND TAG FROM ONE DTD TO ANOTHER VIA STU-III/STU-IIIA/STU-IIIB/STE TELEPHONE CIRCUITS USING JFILL (FILL) - JFILL (FILL) UAS**

NOTE: (U) See the second NOTE following paragraph 10. on page I-6.

a. (U//FOUO) **Sending Operator** performs following steps:

1. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE, using connector cable identified in NOTE following paragraph 9.a., step 1.
2. Call intended receiver using STU-III/STU-IIIA/STU-IIB/STE secure voice mode and inform operator that tagged JTIDS key is to be transferred via JFILL (Fill) - JFILL (Fill) routine.
3. On DTD press Abort.
4. On DTD press “F” or select “Fill” and press ENTR.
5. On DTD press “U” or select “Util” and press ENTR.
6. On DTD press “S” or select “Setup” and press ENTR.
7. On DTD press “P” or select “Protocol” and press ENTR.
8. On DTD press “S” or select “Stu” and press ENTR.
9. On DTD press Abort.
10. On DTD press “X” or select “Xmit” and press ENTR.
11. On DTD press “I” or select “Issue” and press ENTR.
12. On DTD press P UP, P DN and ENTR to select keys to transmit.
13. On DTD press “E” or select “SEND” and press ENTR.
14. On DTD press “D” or select “Direct” and press ENTR.
15. On DTD observe “Connection to Station...” message.
16. On DTD press “SEND”.
17. On DTD observe “STU-III Connection Complete” message.
18. On DTD press “CLR”
19. On DTD observe “Attempting to Connect” message and various other transfer messages.
19. When transfer is complete, disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

b. (U//FOUO) **Receiving Operator** performs following steps:

1. On STU-III/STU-IIIA/STU-IIB/STE acknowledge readiness to receive RED JTIDS key(s) using JFILL (Fill) - JFILL (Fill) routine.

2. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE.
3. On DTD press Abort.
4. On DTD press “F” or select “Fill” and press ENTR.
5. On DTD press “U” or select “Util” and press ENTR.
6. On DTD press “S” or select “Setup” and press ENTR.
7. On DTD press “P” or select “Protocol” and press ENTR.
8. On DTD press “S” or select “Stu” and press ENTR.
9. On DTD press Abort.
10. On DTD press “R” or select “Recv” and press ENTR.
11. On DTD observe “Connect to Station...” message.
12. On DTD press “RCV”.
13. On DTD observe “STU-III Connection Complete” message.
14. On DTD press “CLR”.
15. On DTD observe “Attempting to Connect” message.
16. On STU-III/STU-IIIA/STU-IIB/STE press’ SECURE DATA button.
17. On DTD observe various transfer messages
18. On STU-III/STU-IIIA/STU-IIB/STE when transfer is complete, press SECURE VOICE button.
19. On STU-III/STU-IIIA/STU-IIB/STE acknowledge receipt of transferred JTIDS key(s).
20. Disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

NOTE: (U//FOUO) Key transfer is complete when the Retransmit menu is displayed on transmitting DTD and “Connect to Station” is again displayed on receiving DTD.

NOTE: (U) Sending and receiving operators must record key transfers as required by their respective Services.

12. (U) **TRANSFERRING JTIDS KEY AND TAG FROM ONE DTD TO ANOTHER VIA STU-III/STU-IIIA/STU-IIB/STE TELEPHONE CIRCUITS TRANSMITTING FROM JFILL AND RECEIVING ON CT3 UAS**

NOTE: (U) See the second NOTE following paragraph 10. on page I-6.

a. (U//FOUO) **Sending Operator** performs following steps (using JFILL):

1. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE, using connector cable identified in NOTE following paragraph 9.a., step 1.
2. Call intended receiver using STU-III/STU-IIIA/STU-IIB/STE secure voice mode and inform operator that tagged JTIDS key is to be transferred using JFILL to CT3 routine.
3. On DTD press Abort.
4. On DTD press “F” or select “Fill” and press ENTR.
5. On DTD press “U” or select “Util” and press ENTR.
6. On DTD press “S” or select “Setup” and press ENTR.
7. On DTD press “P” or select “Protocol” and press ENTR.
8. On DTD press S” or select “Stu” and press ENTR.
9. On DTD press Abort.
10. On DTD press “X” or select “Xmit” and press ENTR.
11. On DTD press “I” or select “Issue” and press ENTR.
12. On DTD press P UP, P DN and ENTR to select keys to transmit.
13. On DTD press “E” or select “SEND” and press ENTR.
14. On DTD press “D” or select “Direct” and press ENTR.
15. On DTD observe “Connect to Station...” message.
16. On DTD press “SEND”.
17. On DTD observe “STU-III Connection Complete” message.
18. On DTD press “CLR”.
19. On DTD observe “Attempting to Connect” message and various other transfer messages.
20. When transfer is complete, disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

b. (U//FOUO) **Receiving Operator** performs following steps (using CT3):

1. On STU-III/STU-IIIA/STU-IIB/STE acknowledge readiness to receive RED JTIDS key(s) using JFILL to CT3 routine.
2. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE.
3. On DTD start CT3 application, beginning at RSL Main Menu.
4. On DTD press “R” or select “Recv” and press ENTR.

5. On DTD press “U” or select “Unassigned” and press ENTR.
6. On DTD use P DN and ENTR to select source UNKNOWN.
7. On DTD press “R” or SELECT “RS232 Protocol and press ENTR.
8. On DTD press “N” or select “No” and press ENTR AT DEFAULT PROMPT.
9. On DTD observe “Connect to...” message
10. On DTD press ENTR or Down Arrow key.
11. On DTD observe “Set Desired Position” message prompt.
12. On DTD press ENTR or Down Arrow key.
13. On STU-III/STU-IIIA/STU-IIB/STE press SECURE DATA button.
14. On DTD observe various transfer messages.
15. On STU-III/STU-IIIA/STU-IIB/STE when transfer is complete press SECURE VOICE button.
16. On STU-III/STU-IIIA/STU-IIB/STE acknowledge receipt of transferred JTIDS key(s).
17. Disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

NOTE: (U//FOUO) Key transfer is complete when Retransmit menu is displayed on transmitting DTD and “Connect to Station” is again displayed on receiving DTD.

NOTE: (U) Sending and receiving operators must record key transfers as required by their respective Services.

13. (U) **TRANSFERRING JTIDS KEY AND TAG FROM ONE DTD TO ANOTHER VIA STU-III/STU-IIIA/STU-IIB/STE TELEPHONE CIRCUITS USING CT3 - CT3 UAS**

NOTE: (U) See the second note following paragraph 10. on page I-6.

NOTE: (U//FOUO) If a key tag is transmitted that already exists on the CT3 DTD, an error message offering the user a variety of choices will be displayed. In some circumstances, a rollback and COMSEC error might occur requiring the that the DTD be powered off. This will cause the loss of all data transferred.

NOTE: (U//FOUO) When beginning the actual data transfer, the receiving DTD displays the “Attempting to Connect” message during the time that the transmitting DTD is preparing the data for transfer. The amount of time is variable, depending on the amount of data to be prepared. Although this wait may be longer than the receiving operator may expect, do not disrupt the connection.

a. (U//FOUO) **Sending Operator** performs following steps, using RSL Main Menu:

1. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE, using connector cable identified in NOTE following paragraph 9.a., step 1.
2. Call intended receiver using STU-III/STU-IIIA/STU-IIB/STE secure voice mode and inform operator that tagged JTIDS key is to be transferred using CT3 to CT3 routine.
3. On DTD press “X” or select “Xmit” and press ENTR.
4. On DTD press “D” or select “Database” and press ENTR.
5. On DTD press “U” or select “STU3” and press ENTR.
6. On DTD press “M” or select “Manual” and press ENTR.
7. On DTD press “S” or select “Sel_dbases” and press ENTR.
8. On DTD press “K” or select “Key” and press ENTR.
9. On DTD press “A” or select “All” and press ENTR or press “S” or select “Sel_items” and press ENTR. **NOTE:** If “A” is pressed or “All” is selected, skip to step 12.
10 On DTD use P UP, P DN and ENTR to select keys to transmit.
11. On DTD press “D” or select “Done” and press ENTR.
12. On DTD observe “Preparing...” and “Connect to...” messages.
13. On DTD press ENTR or DN Arrow.
14. On DTD observe “Attempting to Connect” message and various other transfer messages.
15. When transfer is complete, disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

b. (U//FOUO) **Receiving Operator** performs following steps:

1. On STU-III/STU-IIIA/STU-IIB/STE acknowledge readiness to receive tagged JTIDS key using CT3 - CT3 routine.
2. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE.
3. On DTD press “R” or select “Recv” and press ENTR.
4. On DTD press “D” or select “Database” and press ENTR.
5. On DTD press “U” or delect “STU3” and press ENTR.
6. On DTD observe “Connect to...” message.
7. On DTD press ENTR or the DN arrow.

8. On STU-III/STU-IIIA/STU-IIB/STE press SECURE DATA button.
9. On DTD observe various transfer messages.
10. On STU-III/STU-IIIA/STU-IIB/STE when transfer is complete, press SECURE VOICE button.
11. On STU-III/STU-IIIA/STU-IIB/STE acknowledge receipt of transferred keys.
12. Disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

NOTE: (U//FOUO) Key transfer is complete when the Retransmit menu is displayed on transmitting DTD and "Connect to Station" is once again displayed on receiving DTD.

NOTE: (U) Sending and receiving operators must record key transfers as required by their respective Services.

14. (U) **TRANSFERRING ALL JTIDS DATA BASES FROM ONE DTD TO ANOTHER VIA STU-III/STU-IIIA/STU-IIB/STE TELEPHONE CIRCUIT USING CT3 TO CT3 UAS**

NOTE: (U) See the second NOTE following paragraph 10. on page I-6.

NOTE: (U//FOUO) If a key tag is transmitted that already exists on the CT3 DTD, an error message offering the user a variety of choices will be displayed. In some circumstances, a rollback and COMSEC error might occur requiring that the DTD be powered off. This will cause the loss of all data transferred.

NOTE: (U//FOUO) When beginning the actual data transfer, the receiving DTD displays the "Attempting to Connect" message during the time that the transmitting DTD is preparing the data for transfer. The amount of time is variable, depending on the amount of data to be prepared. Although this time may be longer than the receiving operator may expect, do not disrupt the connection.

a. (U//FOUO) **Sending Operator** performs following steps, beginning at the RSL Main Menu:

1. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE, using connector cable identified in NOTE following paragraph 9.a., step 1.
2. Call intended receiver using STU-III/STU-IIIA/STU-IIB/STE secure voice mode and inform operator that all JTIDS data is to be transferred using CT3 to CT3 routine.
3. On DTD press "X" or select "Xmit" and press ENTR.
4. On DTD press "D" or select "Database" and press ENTR.
5. On DTD press "U" or select "STU3" and press ENTR.
6. On DTD press "M" or select "Manual" and press ENTR.

7. On DTD press “A” or select “All_dbases” and press ENTR or press “S” and select “Sel_dbases” and press ENTR. **NOTE:** If “A” or “All dbases” is selected, skip to step 12.
8. On DTD select desired database for transmission.
9. On DTD press “A” or select “All” and press ENTR or press “S” and select “Sel_items” and press ENTR. **NOTE:** If “A” if “All” is selected, skip to step 12.
10. On DTD use P UP, P DN and ENTR to select items to transmit.
11. On DTD use “D” or select “Done” and press ENTR.
12. On DTD observe “Preparing...” or “Standby...” and “Connect to...” messages.
13. On DTD press ENTR or Down arrow.
14. On DTD observe “Attempting to connect” message and various other transfer messages.
14. When transfer is complete, disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

b. (U//FOUO) **Receiving Operator** performs following steps:

1. Respond to sending operator’s call and acknowledge readiness to receive JTIDS data bases using CT3 to CT3 routine.
2. Connect DTD to ATU-III/STU-IIIA/STU-IIB/STE.
3. On DTD press “R” of select “Recv” and press ENTR.
4. On DTD press “D” or select “Database” and press ENTR.
5. On DTD press “S” or select STU3 and press ENTR.
6. On DTD observe “Connect to...” message.
7. On DTD press ENTR of Down arrow.
8. On STU-III/STU-IIIA/STU-IIB/STE press SECURE DATA button.
9. On DTD observe various transfer messages.
10. On STU-III/STU-IIIA/STU-IIB/STE when transfer is complete, press SECURE VOICE button.
11. On STU-III/STU-IIIA/STU-IIB/STE acknowledge receipt of transferred JTIDS data bases.
12. Disconnect DTD from STU-III/STU-IIIA/SUU-IIB/STE.

NOTE: (U//FOUO) Key transfer is complete when the Retransmit menu is displayed on transmitting DTD and “Connect to Station” is once again displayed on receiving DTD.

NOTE: (U) Sending and receiving operators must record key transfers as required by their respective Services.

15. (U) **TRANSFERRING JTIDS KEY AND TAG FROM ONE DTD TO ANOTHER VIA STU-III/STU-IIIA/STU-IIB/STE TELEPHONE CIRCUIT USING FILL UAS**

NOTE: (U) See the second NOTE following paragraph 10. on page I-6.

a. (U//FOUO) **Sending Operator** performs following steps, using the FILL UAS routine:

1. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE, using connector cable identified in NATO following paragraph 9.1., step 1.
2. Call intended receiver using STU-III/STU-IIIA/STU-IIB/STE secure voice mode and inform operator that tagged JTIDS key is to be transferred using FILL UAS routine.
3. On DTD press “U” or select “Util” and press ENTR.
4. On DTD press “S” or select “Setup” and press ENTR.
5. On DTD press “P” or select “Protocol” and press ENTR.
6. On DTD press “S” or select “Stu” and press ENTR.
7. On DTD press Abort.
8. On DTD press “X” or select “Xmit” and press ENTR.
9. On DTD press “I” or select “Issue” and press ENTR.
10. On DTD using P UP, P DN and ENTR to select keys to transmit.
11. On DTD select “SEND” and press ENTR.
12. On DTD press “D” or select “Direct” and press ENTR.
13. On DTD observe “Connect to Station...” message.
14. On DTD press “SEND”.
15. On DTD observe “STI-III Connection Complete” message.
16. On DTD press CLR.
17. On DTD observe “Attempting to Connect” message and various other transfer messages.
18. When transfer is complete, disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

b. (U//FOUO) **Receiving Operator** performs following steps:

1. On STU-III/STU-IIIA/STU-IIB/STE acknowledge readiness to receive tagged JTIDS key using FILL UAS routine.

2. Connect DTD to STU-III/STU-IIIA/STU-IIB/STE.
3. On DTD press “RCV”.
4. On DTD observe “STU-III Connection Complete” message.
5. On DTD press “CLR”.
6. On DTD observe “Attempting to Connect” message.
7. On STU-III/STU-IIIA/STU-IIB/STE press” SECURE DATA key.
8. On DTD observe various transfer messages.
9. On STU-III/STU-IIIA/STU-IIB/STE when transfer is complete, press SECURE VOICE button.
10. On STU-III/STU-IIIA/STU-IIB/STE acknowledge receipt of transferred keys.
11. Disconnect DTD from STU-III/STU-IIIA/STU-IIB/STE.

NOTE: (U//FOUO) Key transfer is complete when Retransmit menu is displayed on transmitting DTD and “Connect to Station” is again displayed on receiving DTD.

NOTE: (U) Sending and receiving operators must record key transfers as required by their respective Services.

THIS PAGE IS INTENTIONALLY BLANK

(U) FIELD GENERATION AND OVER-THE-AIR DISTRIBUTION OF COMSEC KEY IN SUPPORT OF TACTICAL OPERATIONS AND EXERCISES