CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6 CJCSM 6520.01B
DISTRIBUTION: A, B, C 28 April 2015

LINK 16 JOINT KEY MANAGEMENT PLAN

Reference(s):
See Enclosure C for references.

1. Purpose. This manual outlines procedures for production, distribution, and use of Link 16 COMSEC keying material (KEYMAT) for legacy and crypto modernized Link 16 systems in accordance with references a through i. Enclosure A contains the Link 16 Joint Key Management Plan, and Enclosure B provides the Link 16 COMSEC Entities Contact List. The Joint Multi-Tactical Data Link (TDL) Operating Procedures manual (reference a) provides further guidance regarding operational management of Link 16 and other tactical data links. References b, c, and d contain National Security Agency (NSA) security doctrine associated with Link 16 devices.

2. Superseded/Cancellation. This document supersedes CJCSM 6520.01A, 9 December 2011, Link 16 Joint Key Management Plan, for crypto modernized Link 16 systems.

3. Applicability. This manual provides guidance to the Services, Combatant Commanders, unified commanders, and Defense Agencies involved in the production, distribution, or use of Link 16 KEYMAT for Link 16 systems.

4. Procedures. This manual documents current key management procedures and the procedures applicable to the Electronic Key Management System (EKMS) and the Key Management Infrastructure (KMI) as implemented.

5. Summary of Changes. CJCSM 6510.01B addresses both Link 16 terminals that have been crypto modernized and terminals that have not yet been crypto modernized.

6. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET. DoD Components (to include the Combatant Commands), other Federal Agencies, and the public) may obtain copies of this directive through the Internet from the CJCS Directives

Electronic Library at <http://www.dtic.mil/cjcs_directives>. JS activities may also obtain access via the SIPR Directives Electronic Library Web sites.

7. Effective Date. This MANUAL is effective upon receipt.

JACQUELINE D. VAN OVOST, Maj Gen, USAF
Vice Director, Joint Staff

Enclosures
- A - Link 16 Joint Key Management Plan
- B - Link 16 COMSEC Entities Contact List
- C - References
- GL - Glossary

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

LINK 16 JOINT KEY MANAGEMENT PLAN

1. General Information

a. Background

(1) Link 16 is the DoD and North Atlantic Treaty Organization (NATO) primary tactical data link for Service and Defense agency C2, intelligence, and in some cases, weapons systems applications. It is a secure, jam-resistant data link primarily using the Joint Tactical Information Distribution System (JTIDS) (AN/URC-107 Series), Multifunctional Information Distribution System (MIDS) Low-Volume Terminal (LVT) (AN/USQ-140 Series) sets, and MIDS Joint Tactical Radio System (JTRS) sets. There are also several form factor versions of Link-16 equipment that are in development with reduced volume in size to fit into missiles, small ships, helicopters, and manpacks.

(2) Link 16 supports functional mission areas including joint theater air and missile defense, attack operations, counter-air, interdiction, suppression of enemy air defenses, close air support, and time-critical targeting prosecution. Link 16 networks may include allied or coalition forces and are protected by COMSEC equipment and KEYMAT.

(3) Due to the nature of coordinated Link 16 networks, KEYMAT will normally be generated and distributed by EKMS or KMI as described in section A.2 and A.3. Link 16 system KEYMAT currently entered into the Link 16 terminal using a standard fill device. However, after Crypto modernization some of the older fill devices will become obsolete and will not support Link 16 terminals. Some KEYMAT may be generated locally by COMSEC Accounts supporting operational forces that may need a unique KEYMAT to support an ad-hoc Link 16 network or Link 16 Network Participation Group (NPG) for training, exercise or specialized operations.

b. Transition to Modernized Crypto

(1) CJCSI 6510.02D directs DoD to perform Link 16 Crypto Modernization for all DoD users and must also be extended to Allied and Coalition partners. This modernization project is a major production and deployment project across all of DoD and will take several years to accomplish. Link 16 terminals that have been modernized will be backwards compatible with legacy terminals. Crypto modernization for Link 16 was carefully structured to support operational employment of Link 16 equipment while maintaining compatibility with legacy Link 16 equipment.

(2) The Link 16 architecture internally manages keys by assigning them a Cryptographic Variable Logic Label (CVLL). Externally, a key Short Title is assigned to a CVLL by the Joint Interface Control Officer (JICO) via an Operational Tasking Data Link (OPTASK LINK) Message. The network parameters loaded with an Initialization Data Load (IDL) in the Link 16 equipment established how these CVLL are to be used by the network. In the modernized equipment the key is internally tied to the CVLL directly. In the legacy equipment, the key is internally tied to a memory location and the memory location is tied to the CVLL via an internal table. Some operational strategies and procedures manipulate this CVLL table to minimize the number of networks that the host platform has to have. The host platform is designed to take advantage of being able to manipulate the CVLL table and keep the number of network IDLs to load to a minimum (normally two).
The loading of keys is different between the legacy and the modernized equipment. Additionally, operations of platforms with legacy and modernized Link 16 equipment in the same network requires careful planning by the Commander.

c. System Description

(1) Overview. Link 16 Radio Frequency (RF) terminals communicate using a Time Division Multiple Access (TDMA) architecture operating on multiple frequencies in the range of 960-1215 MHz. Link 16 transmissions are encoded in accordance with the "J" series message format defined in Military Standard (MIL-STD) 6016. Due to the operating frequency, Link 16 transmissions are line-of-sight and capable of operating at a range of 300 nautical miles (nm) or an extended mode at a range of 500 nm. This range can be further extended through the use of relay platforms. Link 16 transmissions are protected by encryption devices in the terminal or aircraft electronic systems. Link 16 uses two types of encryption including TRANSEC and Message Encryption (MSEC) and thus requires two crypto variables for a Partitioned Variable Mode (PVM) NPG or one variable for CVM NPG.

(2) Hardware. Table A-1 describes Link 16 terminals and associated platforms. In addition, Link 16 capability is embedded into the systems architecture of the F-22A Raptor and the F-35 Lightning II.

Table 1. Link 16 Terminals, Users, and Associated Platforms

Terminal	Size	Power	Users	Platforms
JTIDS Class 2	1.6 cu ft 130 lb	200 W	USAF USMC USN	COMPASS CALL JSTARS MCE SENIOR SCOUT And other variants ADCP EP-3
JTIDS Class 2H	3.25 cu ft 220 lb	200 W and1000 W with +HPA	USAF USN	AWACS And other variants AEGIS CG/DDG CVN/LHD/LCC E-2C
JTIDS Class 2M	1.3 cu ft 89 lb	40/200 W	USA	PATRIOT JTAGS ADTOC SHORAD THAAD
MIDS-LVT(1)	0.61 cu ft 65 lb	1/200 W and 1000 W with +HPA	USN NATO FMS	EF-18 P-8A EP-3 P-3C (SP) P-3C AIP+ P-8A NHPS Asset X EA-6B MH-60R/S
MIDS-LVT(2)	1.35 cu ft 80.9 lb	25/200 W	USA	PATRIOT THAAD ADAM Cell NOTE: No J-Voice
MIDS-LVT(3) (FDL)	0.61 cu ft 45 lb	50 W	USAF	F-15 ROBE And other variants NOTE: No J-Voice
MIDS-LVT(4)	0.61 cu ft 65 lb	1/25/200 W +HPA Interface	USAF	LAK BCS-M CAC2S NORAD RAIDER GTACS AWACS (planned)

Table 1. Link 16 Terminals, Users, and Associated Platforms (Continued)

Terminal	Size	Power	Users	Platforms
MIDS-LVT(5)	0.61 cu ft 65 lb but embedded in chassis	1/200 W and 1000 W with +HPA	USN	MIDS On Ship (MOS) on Multiple USN platforms
MIDS-LVT(6)	0.61 cu ft 65 lb	1/25/200 W + HPA Interface	USAF	F-16 AC-130 And other variants
MIDS-LVT(7)	0.61 cu ft 65 lb	1/25/200 W + HPA Interface	USAF	B-2 and other variants
MIDS-LVT(11)	1.35 cu ft 80.9 lb	25/200 W	USAF USMC	Pocket J And other variants TAOC MTAOM CDLS UAS CAC2S
MIDS JTRS	0.61 cu ft 65 lb	1/25/200 W	All Services	All USN and USMC F/A-18 E-2D EF-18 G Link Monitoring and Management Tool (LMMT) AWACS (planned) JSTARS Rivet Joint Compass Call
AMF JTRS	252 cu in 16.5 lb	50 W	US Army	Apache
Network Enabled Weapons Strike Common Weapon Data Link KOR-8 (SCWDL)	80 cu in	45 W	USAF USN	Joint Standoff Weapons JSOW C1, SMD II GBU-39/B, Tactical Tomahawk
KOR-24 Small Tactical Terminal (STT)	0.2 cu ft 20 lb	50 W	All Services	Dismounted/ Disadvantaged users
Sea Harrier (SHAR) AN/URC-138	0.53 cu ft 39.8 lb	200 W	GBR	Sea King

Table 1. Link 16 Terminals, Users, and Associated Platforms (Continued)

Terminal	Size	Power	Users	Platforms
F-22 CNI	NA	Receive Only	USAF	F-22A Raptor
AN/ASQ-242	NA	25/200 W	All Services	F-35 Lightning
TacNet Terminal Radio (TTR) (KOV-68)				Possibly used for Weapon Data Link
Small Tactical Terminal (KOR-24)	5 x 5.6 x 9 in; 16.5 lb	50 W	USAF USN	Possibly used for Weapon Data Link

(3) Transmission Characteristics

(a) TDMA. The TDMA transmission structure decomposes data into message sets transmitted during pre-planned intervals (time slots). Each participating terminal is allocated time slots to transmit, receive, or relay data. When the terminal is set to operate in Mode 1 then within each time slot, radio terminal transmission/reception "hops" among 51 discrete frequencies to improve jam resistance. In some cases, a reduced hop set of frequencies may be used when mandated by spectrum authorities. This pseudo-random frequency-hopping sequence is determined by the key used for message and/or transmission security. When the terminal is set to operate in Mode 2, there is no frequency hopping. (Currently there are no known users of Mode 2.) Further information regarding the Link 16 waveform may be found in the MIDS System Segment Specification.

(b) Time Slot. A time slot is a standard interval (7.8125 msec) assigned to individual Link 16 participating units for message transmission and reception. With the exception of voice, round-trip timing (RTT), and free text, data transmitted within a time slot is composed of three, six, or twelve 70-bit words, depending on the packing structure used. A terminal may have enhanced throughput, in which case, more TDL words can be transmitted in a slot. The design of the network establishes the assignment of transmit and receive time slots to each participating platform.

(c) Network Participation Groups (NPGs). NPGs are the basic Link 16 communication "circuits." Each Link 16 network design assigns time slots within NPGs based on the type of information being exchanged. NPGs include net entry, precise participant location and identification (PPLI), RTT, network management, mission management, surveillance, imagery, electronic warfare, and voice. Messages produced by host combat systems are routed for transmission to specific NPGs. Since terminals provide NPG filtering and selection, message assignment by NPG may be used for partitioned security and selective filtering.

(4) Network Management

(a) Network Selection. Link 16 networks are utilized based on the theater data link architecture or operational and training requirements. Operational architectures normally require use of a US joint or allied operational key. Training architectures may require the use of a specialized key.

(b) Network Deconfliction. A Link 16 network is a group of participants in time synchronization and exchanging information. Planning is required to ensure that different networks (encompassing different participants and/or purposes) do not cause mutual interference. The primary way to ensure successful independent network operations is to use different keys (cryptographic differentiation) such that synchronization cannot be achieved between two different networks. The use of different keys (i.e., a different short title) is the preferred method for resolving independent networks. Network time offset (the practice of deconfliction by sending a time to the Link 16 equipment for operational use that is not Coordinated Universal Time (UTC)) is a practice that should not be used. If a command decides to actually use network time offset as the only workable solution for a mission, it must request a waiver from the Joint Staff (js.pentagon.j6.list.dd-c4-cyber-c4t-div-mil@mail.smil.mil). Waivers will be updated annually. The amount of network time offset should be forward from UTC, but not to exceed 1 hour. And a platform after using time offset of a specific amount of time and is required to return to UTC, the platform shall wait the same amount of time before becoming operational using the UTC time. If all platforms of a taskforce have been modernized, network time offset for that taskforce shall not be used. Link 16 terminal upgrades being implemented may not tolerate time offset. Concurrent Multi-Net (CMN) will not work with terminals with standard UTC and time offsets together. Other Link 16 terminal upgrades, combined with KMI will provide for a more efficient method of deconfliction than time offset and have surpassed all the value that time offset has provided in the past.

d. Security. Link 16 circuits may be used to transmit information up to and including SECRET. Link 16 has been evaluated and is approved by the Director, NSA, for operation in the SECRET HIGH security mode if all network participants are cleared for SECRET and have access approval for all information in the Link 16 net. NSA has also assessed Link 16 for the exchange of compartmented and special access information. Although NSA cannot currently certify Link 16 for operation in compartmented mode, segregation can be accomplished by using a separate key for a specific NPG. Because of these information segregation features, a particular designated accrediting authority or certifying authority can, after their own risk assessment, authorize Link 16 for exchange of compartmented or special access information (up to TOP SECRET HIGH) associated with their program. The full cryptographic and information segregation feature of Link 16 should be

used. Each program must evaluate alternatives and specify procedures (e.g., special key, special messages, or additional encryption). All personnel authorized uncontrolled access to Link 16 terminal areas must be cleared at least to the classification level of the Link 16 data being exchanged. Link 16 terminals currently use a variety of cryptographic solutions, called out in the terminal specifications as a secure data unit (SDU), which are all cryptographically compatible. The SDU provides both transmission security (TRANSEC) and communications security (COMSEC) for message security (MSEC).

(1) TRANSEC. Each Link 16 terminal can operate on any one of 127 selected nets with each net defined by a distinct pseudo-random frequency-hopping pattern, increasing resistance to jamming and exploitation. PVM adds another 127 hopping patterns. If two platforms are transmitting with the same key and same time slot number but different cryptographic modes (Common or Partitioned), they will have different hopping patterns. TSEC assignment is one of the Link 16 network initialization parameters and, together with the time slot number, determines the hopping sequence for each net and provides symbol interleaving, pulse modulation encryption, carrier frequency hopping, and message start jitter generated from a key used for TSEC.

(2) MSEC. Link 16 messages are transmitted via data blocks and encrypted using an MSEC key assigned by the Link 16 network initialization parameters. Traffic Encryption Keys (TEKs) provide Link 16 MSEC. Also Link 16 design allows for the use of TEKs not tied to a TSEC operation by using the PVM.

e. KEYMAT. Traffic Encryption Key (TEK) is used for all transmission security (TSEC) and message security (MSEC) operations. The TEK used in legacy equipment is also used in modernized equipment for interoperability. A standard Key Encryption Key (KEK) type is used to encrypt and decrypt TEK in legacy equipment during distribution, issue and key loading to decrease risk of exploitation. Modernized Link 16 algorithms use a new TEK type specified by the NSA document “Key Specification for the Link-16 Family of Equipments.” The new TEK types are normally encrypted by any appropriate KEK types during distribution, issue and key loading to decrease risk of exploitation. Link 16 equipment supports encrypted (black) key fill. The KEK specification is included in the NSA document “Key Specification for the Link-16 Family of Equipments.” All over the air transmissions of a Link 16 system shall be protected by SECRET or, with approving authority, TOP SECRET keys. The Link 16 equipment is designed to support NSA’s policy that all TEK keys shall be filled as black key.

(1) Traffic Encryption Key (TEK). TEK is the key type for encrypting operational message traffic. For Link 16 TEK key type is used for both TSEC

and MSEC operations. The Transmission Security Key (TSK) key type is not used in Link 16.

(2) Key Encryption Key (KEK). A goal of KMI and EKMS is to minimize direct human access to KEYMAT. One strategy used to protect KEYMAT from exploitation is encryption using KEK. The modernized Link 16 equipment will support the different types of KEKs described in the NSA document "Key Specification for the Link-16 Family of Equipments," Table A-2 describes the different uses of the KEKs in the Link 16 system. The Transmission KEK (TrKEK) identified in Table A-2 is part of the EKMS or KMI system and is not directly used by the Link 16 equipment.

Table 2. KEK Types

KEK	**Protected Material**	**Protected Path**	**Specific Protected Material**	**KEK Account/Load**	**KEK Production Location**
ECU KEK For TEKs	Individual keys	From the fill device to SDU	Link 16 TEKs,	Normally pre-loaded into the SDU as part of a mission key load	At Tier 0 or KMI or EKMS system
ECU KEK For KEKs	Individual keys	From the fill device to SDU	Link 16, ECU KEKs	Normally loaded offline as part of integrating platform into a taskforce.	At Tier 0 or KMI or EKMS system
TrKEK	Individual keys	From Key distribution system	Link 16 ECU KEKs, TEKs	Normally preloaded into the fill device	At Tier 2

(a) End Cryptographic Unit (ECU) KEK. ECU KEK is installed in the SDU. The encrypted key obtained from using the ECU KEK is an ECU encrypted key. ECU encrypted keys are received through the fill port or in some cases from the platform host. NSA policy states that ECU KEKs used for encrypting KEKs are not allowed to encrypt TEKs and ECU KEKs used for encrypting TEKs are not allowed to encrypt KEKs. Since the Link 16 equipment cannot enforce this policy, it must be enforced by good COMSEC Material System (CMS) training. KMI may be built to enforce this policy.

(b) Transmission Key Encryption Key (TrKEK). This KEK is installed in the Tier 3 fill device (i.e., AN/PYQ-10 Simple Key Loader (SKL) or KIK-20 Secure Data Transfer Device 2000 System (SDS)). The key distribution system (KMI or EKMS) encrypts keys for the user in a TrKEK. The encrypted keys protected by this TrKEK are referred to in this document as fill device encrypted keys. The fill device uses the TrKEK to decrypt the fill device encrypted keys prior to loading into an SDU. For the purposes of this

document, TrKEK describes KEKs used to encrypt individual keys for the fill device which will decrypt the keys in the ECU fill process.

(3) Key Availability. Link 16 COMSEC is established through use of either the CVM, one crypto variable used for both TSEC and MSEC, or the PVM, in which two crypto variables, one for TSEC and one for MSEC. Coordinated joint operations require that different platforms use the same TEK short titles and coordinate with each service's network design facility to supply the IDL parameters for the platforms. Link 16 is structured to support multiple cryptonets using different TEKs (i.e., it can use more than one short title at a time), and the legacy system is capable of smoothly operating on four cryptonets simultaneously. After Link 16 modernization, the Link 16 can be initialized to operate on up to 32 cryptonets simultaneously. Although no maximum limit on the number of platforms that can be on any single cryptonet is prescribed for Link 16 TEK cryptonets, this number should be as small as operationally feasible. To minimize the risk of global compromise, the same TEK short title must not be used worldwide. Since limiting the distribution of keys to facilitate groups may lead to unforeseen operational difficulties, the Joint Staff has authorized the Joint Communications Security Management Office (JCMO) to distribute to each COMSEC account access to a worldwide key for emergency and contingency operations. Numerous non-emergency or contingency TEKs are available for each regional combatant command which shall be used for missions that can be adequately planned in advance. Each command may use its collection of short titles as operationally required. Section A.2 "Key Ordering Parameters for KMI and EKMS" describes the procedures followed by combatant commands when ordering short titles. The key distribution system generates and distributes keys to authorized accounts in accordance with the account's reserve-on-board (ROB) requirements. Some COMSEC Accounts hold the key for Tier 3 local elements. Availability of required keys at these COMSEC Accounts or EKMS/KMI Accounts provides servicing facilities rapid distribution to the Tier 3 accounts. Combatant commands should include Link 16 key distribution in operational and contingency plan development.

(4) Key Types. Since the Link 16 key is available in either unencrypted or encrypted format. Associated with each encrypted key is a KEK which had to be generated, distributed, and issued along with the encrypted form. The encryption of a key should be done at the lowest practical tier. ECU encrypted keys, both TEK and KEK, shall be used wherever possible. In order to comply with Information Assurance Directorate (IAD), IAD Management Directive 10, Revised 15 July 2011, only encrypted TEK shall be loaded into a Link 16 system. Either encrypted or unencrypted ECU KEK may be loaded into Link 16 systems. TEKs may be encrypted by NSA or locally encrypted by the COMSEC account Local Management Device/Key Processor (LMD/KP) or KMI Management Client (MGC) workstations. The intent is meet IAD MD10 by protecting the TEK from its original generation point all the way to the ECU,

with unencrypted TEK never being accessible outside of the ECU, KP or MGC. Encryption of unencrypted keys is the responsibility of the commander at the lowest distribution element capable of encryption. The KEK is used to protect the movement of an underlying unencrypted key from the local key distribution point to the using ECU. The command encrypting a key is responsible for managing KEK distribution to the ECU for decryption of the ECU encrypted keys.

(a) Operational Keys. These keys are used to support operational missions. They are classified at least SECRET CRYPTO and change each cryptographic period. Operational keys are designated for special mission use or for a specific combatant command.

(b) Maintenance Keys. These global keys are used to support maintenance. They are For Official Use Only. Maintenance keys are also used in training, research, development, test, and evaluation.

(c) Test Keys. These keys are used to conduct "on-the-air" testing under operational, training and demonstration conditions. They are SECRET keys that change for every cryptographic period (global, but not necessarily pre-positioned). An operational key may also be used for test purposes within the valid cryptographic period for that key. Normally, operational keys should be used if the data transmitted has operational value.

(5) Operational Key Allocation. Link 16 requires several operational keys, which are described below.

(a) Emergency Contingency Operational Key. One set of joint keys will be maintained for worldwide emergency contingency use. This set will be held by all Link 16 user COMSEC accounts and used only under direction of the Joint Staff to support an emergency in which users from different combatant AORs must arrive in a theater of operations on short notice. The JCMO orders the short titles of operational keys for such an emergency contingency operation. The number of emergency and contingency operational keys to be held by the JCMO office is determined by the Joint Staff. The number of short titles should be sufficient to support unexpected or emergency operational requirements that have not been planned for, realizing that operational nets currently use two or three TEKs.

(b) Joint Theater Key. This key is used for operations among US commands within a theater of operations. During normal operations, a separate set of short titles will be used for each combatant command. If units from a supporting combatant command are involved, they will obtain the key via the supported commander as part of the normal planning process. Availability of five short titles provides flexibility and the potential for multiple cryptonets. If more keys are needed they can easily be ordered.

(c) Allied Keys. These keys are used within an area of operations that includes Allied elements. During normal operations, a separate set of short titles will be used for each combatant command. Units from a supporting command that are involved in operations will obtain keys via the supported combatant commander as part of the normal planning process. Allied key distribution may also require NSA to distribute keys outside of EKMS. It may also require Service Acquisition Program Offices to program for Coalition Electronic Key Management System (C-EKMS) installation, operations, and maintenance as well as connectivity to Tier 2 accounts of the supported combatant command (COCOM) for electronic KEYMAT distribution to coalition partners not part of NATO or Combined Communications Electronics Board (CCEB). Refer to Table A-5 (Operational Link 16 Key Allocation) and Enclosure B (Link 16 COMSEC Entities Contact List) to determine which Tier 2 account to contact.

(6) Cryptographic Period. TEK and ECU KEK are distributed using the following edition/segment convention.

(a) TEK. Each TEK edition has a one-month supersession rate, and each TEK segment has a one-day cryptographic period. The TEK supersession rate begins at the beginning of the first minute defined by UTC and ends at the end of the last minute defined by UTC. This crypto period convention is an integral part of the Link 16 architecture. A TEK supersession rate shall not be extended except in cases in which the Link 16 terminal has been initialized in the seven-day mode. The seven-day mode is a capability of the Link 16 equipment; however, NSA recommends not using it unless it can be justified. The current infrastructure is not designed to support the seven-day mode in Link 16 without significant, complex workarounds. Explicit coordination and a joint Service agreement are required to use a seven-day supersession rate. Although all Link 16 terminals are capable of operating in a seven-day mode, many platform C2 systems are not. If one Link 16 unit in a net uses the seven-day mode, all network participants must operate in the seven-day mode. Seven-day mode is not interoperable with one-day mode.

(b) ECU KEK. Each ECU KEK edition used for TEK encryption normally has a six-month supersession rate, and each ECU KEK segment has a one-month supersession rate. When a Link 16 ECU KEK is generated, the cryptographic period is prescribed to coincide with the number of editions of TEK that it encrypts/decrypts. Some remote rekey requirements may use ECU KEKs that have segments with a crypto period of six months, a year, or more. ECU KEKs used to encrypt other KEKs will have a crypto period not to exceed 1 year.

f. Secure Data Unit. Link 16 terminals use a cryptographic solution that makes them cryptographically compatible. Specific Link 16 system cryptographic solutions include various types of SDUs and supporting

equipment. The number of traffic keys that the legacy SDUs may store is 8 keys. After the Link 16 modernization, the SDU can store a 1000 traffic keys. The COMSEC key loading protocol is distinguished by the various types of SDUs.

(1) SDU Types. SDUs are divided into the following three major categories based on common functional characteristics.

(a) JTIDS KGV-8(E-2), KGV-8A, KGV-8C, and E-GLD. These devices can store and use only TEK and Over-the-Air Rekeying (OTAR) KEK. Eight random access memory (RAM) locations are available for daily use key storage. These SDUs are keyed via Data Standard (DS) 102 protocol and can receive keys only in the unencrypted form from the fill device. An external keyer control panel (KCP) or load control unit (LCU) is required to manually select the desired memory location for the key fill process. All keys stored in RAM are non-extractable and are erased when power is removed from the SDU. At the completion of the crypto modernization update of Link 16 systems, all of these devices will be replaced by a new cryptographic solution as part of the JTIDS Product Improvement (JPI).

(b) JTIDS KGV-8B and JTIDS/MIDS LVT COMSEC/TRANSEC Integrated Circuit DS-101 Hybrid (CDH). These devices can be filled with either unencrypted or encrypted TEK in any of 8 (or 64 for MIDS-LVT(2)) RAM storage locations. All keys are stored in unencrypted form. Encrypted keys are decrypted by their associated pre-loaded KEK prior to storage in RAM. Nine electronic erasable programmable read-only memory (EEPROM) locations are available for KEK storage. Keys stored in EEPROM are also stored in unencrypted form. All keys stored in RAM or EEPROM are protected from extraction and exploitation by other means. All keys stored in RAM are erased when power is removed from the SDU. Keys stored in EEPROM can be erased only upon receiving an external command from a SKL, SDS, or fill device. These SDUs are filled via the DS-101 protocol and do not require a KCP. A fill device running the Common Tier 3 (CT3) compatible fill device user application software (UAS) or the JTIDS Fill (JFILL) device key management software provides the correct DS-101 loading information to set the SDU location into which the key is to be stored. A data management system such as the SKL, iAPP, Joint Mission Planning System (JMPS), Automated Communications Engineering Software (ACES) or the Data Management Device (DMD) is required to format and load encrypted TEK, distributed by EKMS Tier 0 or Tier 2, into a fill device.

(c) Programmable COMSEC. Systems such as MIDS JTRS, Small Tactical Terminal (STT), F-22A and F-35 use organic embedded programmable COMSEC solutions to support Link 16. These devices can be filled with encrypted and unencrypted TEK. They can store many days, or months of TEK. Internal key management functionality allows these systems to select the

correct TEK for the correct crypto period, CVLL, network, and NPG. These systems also require a data management system such as JMPS, ACES, iApp, or DMD to format and load encrypted TEK. When KMI is available, the KMI Intermediary Application (iApp) can be used instead of the DMD or ACES. In addition, some programmable COMSEC systems require ACES, DMD, or iApp to provide tagging information to the fill device for encrypted or unencrypted key loading.

(2) Characteristics. SDUs are distinguished by the number of keys they may store and the COMSEC key loading attributes. Table A-3 shows a sampling of Link 16 terminal types and their associated SDUs.

Table 3. Link 16 Terminal/SDU Use

Terminal	SDU	Key Storage
JTIDS Class 2	KGV-8, KGV-8A/C KGV-8B[1], CSP	8 keys/DS-102 8 keys/DS-101
JTIDS Class 2 (After JTIDS Product Improvement (JPI))	KGV-80 Programmable JTIDS COMSEC Module (JCM) embedded on JTIDS Signal Message Processor (JSMP)	1000 keys/DS-101
MIDS LVT(all variants except LVT2)	U TVB-CDH or KOV-55 LCM embedded on SMP Card[1]	8 keys/DS-101[2]
MIDS LVT2	U TVB-CDH embedded on SMP Card[1]	64 keys/DS-101[2]
MIDS LVT (all variants after Block Upgrade 2 (BU2))	Programmable KOV-55 LCM embedded on Signal Message Processor (SMP)	1000+ keys/DS-101
MIDS JTRS	Z BAS-MIDS JTRS Programmable, Scalable Information Assurance Module (PSIAM) Crypto Sub-System (CSS), Embedded programmable crypto	1000+ keys/DS-101
STT	Embedded programmable COMSEC Module	1000+ keys/DS-101
SHAR	CDH embedded on Signal Message Processor (SMP)	8 keys/DS-101

[1] The DS-101 ECU, such as the KGV-8B and CDH, may be filled with an ECU encrypted key that uses an ECU KEK for encryption and decryption.

[2] The Common Signal Processor (CSP) (CDH) can be installed as either DS-102 or DS-101. There are switches on the card itself to select which protocol will be used.

(a) Fill Port. The SDU fill port is designed in accordance with the Interoperability Standards for Electronic Key Management Systems 308 protocol standard. Keys can be loaded into the E-GLD, KGV-8(E-2), KGV-8A, and KGV-8C using the common fill device interface protocol (commonly referred to as DS-102). Keys can be loaded into the KGV-8B, CDH, and

programmable COMSEC using the DS-101 data packet exchange protocol as limited and augmented by NSA Specification 90-2A.

(b) Cryptographic Periods. Link 16 KEYMAT cryptographic periods extend from beginning of the first minute of the day defined by UTC to the end of the last minute of the day as defined by UTC.

(c) Cryptographic Engine. JTIDS, MIDS, MIDS JTRS, STT, TTR, and SHAR Link 16 terminals use an SDU with an integrated Crypto based message security/transmission security as the primary cryptographic engine. The crypto encrypts and decrypts messages for each time slot. Although the SDU can use the same key for generating the bits used for TSEC as well as for MSEC, a different key may be used for MSEC if desired. Normally the system switches the key to be used from that used for the current day to those reserved for the next day at rollover. At the end of the last minute of the day as defined by UTC, the terminal triggers the SDU to switch to the next day's keys and erase previously used keys. Programmable COMSEC Link 16 systems use the new algorithms specified by the "THORNTON Crypto Mod Cryptographic Synchronization" specification. The only differences in capabilities are that the programmable COMSEC systems can store many more keys, and are not limited to current and next day functionality.

(d) Automatic Rollover. Unlike systems that require key loading at the change of each cryptographic period (e.g., daily), Link 16 is designed to automatically roll over to a new key at the end of each cryptographic period. Link 16 rollover occurs at the end of the last minute of the day as defined by UTC.

(e) SDU Pairs. The Link 16 system is designed to set up today's keys and tomorrow's keys. At rollover it stops using the keys it is currently using and begins to use the next day's keys. It zeroizes the keys it finished using and loads the keys for the following day. The modernized Link 16 system can be filled with enough keys to last for a mission of several days. Keys for successive cryptographic periods are loaded into the crypto engine ready for use. This relieves the system operator from loading a new key or performing a manual switch. Keys may be loaded for the next cryptographic period at the operator's convenience. At the end of the next cryptographic period, the terminal begins using the next key and erases the previous key. To keep the Link 16 in continuous operation, key fill for these terminals must take place before the filled keys run out. Internal key management functionality allows these systems to select the correct TEK for the correct crypto period and NPG. The legacy Link 16 allows for the loading of two days of crypto keys at a time: Current day and next (second) day pairs. At rollover the terminal switches to the next (second) day key. Once the terminal switches to the next day key, the previous days key is zeroized and the key now being used becomes the current day key. Any time during the current day a key for the next day can be loaded.

The fill device has been programmed to keep track of current and next day keys during crypto day change. The fill device will load the correct key in the correct location during the fill process. The fill device will actually load current day keys and the next day key pairs. The process is more complicated than this verbiage indicates. The fill device calculates which keys are to be loaded based on the assumption that the terminal has been set with the correct Common Crypto Period Designator (CCPD) value and the correct Crypto Period Designators (CPDs) in the CVLL table. A human operator is responsible for selecting the correct CCPD for the terminal. In the modernized Link 16 all these calculations have been moved to the Link 16 terminal and no human operator is involved.

(f) SDU Pairs Details of Legacy Link 16 SDU Location Pair processing. Legacy Link 16 utilizes its SDU RAM storage locations in pairs (0/1, 2/3, 4/5, 6/7). Keys for successive cryptographic periods are loaded into each pair. If the terminal is using a key in SDU RAM location 0, the terminal begins using the key in location 1 at rollover and will erase the key in location 0. This relieves the system operator from loading a new key or performing a manual switch. Keys may be loaded for the next succeeding cryptographic period at the operator's convenience. At the end of the next cryptographic period, the terminal begins using the key in location 0 (provided a new key has been loaded) and erases the key in location 1. The same procedure applies for pairs 2/3, 4/5, and 6/7. The Link 16 terminal is required to roll over all the locations in the same way, from even to odd or odd to even (the terminal will not roll over a 0 to a 1 and at the same time, a 7 to a 6). To keep the Link 16 in continuous operation, key fill must take place daily. It is imperative that successive key fill take place before the second rollover. For modernized Link 16 terminals the keys to be used for today and tomorrow are selected, retrieved, and activated by a key management function in the terminal based on effectivity of the keys, CVLLs, and waveform instance ID. At rollover, the next day's keys are selected, retrieved, and activated.

g. Key Loading Devices. COMSEC key loading devices that support Link 16 include the data transfer device (DTD), SKL, SDS, and other modern fill devices. The SKL and SDS are used to load the DS-101 protocol into the SDU. Eventually other special purpose fill devices may be added to this list; such as the Tactical Key Loader (TKL), Really Simple Key Loader (RASKL), and Next Generation Load Device type. The key is loaded into the fill device using the KMI iApp or EKMS Tier 2 workstation.

(1) Fill Device Preparation. Prior to loading the SDU, the fill device UAS is set up for the specific SDU. The fill device UAS supports Link 16 by providing an automated set of procedures for assistance in loading a key. Optimally, the UAS allows the user to press one button on the keypad to initiate key loading. Specific identifying data is associated with each SDU in the form of a station identifier (STATION ID) and a station bus address

(STATION ADDRESS) for use in single point keying configurations. A Personal Computer (PC)-based UAS provides users with an automated means of gathering, collating, and formatting the data for transfer to the fill device using either an RS-232 serial, Universal Serial Bus or high-level data link control protocol. The data includes key tag, cryptographic period, classification, a unique text identifier (TEXT ID) and effective date information for the required keys, SDU RAM or EEPROM storage location, and a unique terminal/ equipment STATION ID. Additionally, data obtained from the OPTASK LINK message (i.e., key short title, SDU memory location, cryptographic period) is transferred from the PC to the fill device. Data is transferred from the PC to the fill device before or during key transfer. Provisions are available for manual entry of identifying data directly into the fill device.

(a) The modernized COMSEC Link 16 systems can also receive network identification information (Network Name), effectively date/time, and key usage information: CVLLs. The CVLLs are used for internal system key management.

(b) Only after the identifying data has been transferred to the fill device can keys be loaded into the Link 16 SDU. Keys are loaded into a fill device from a Tier 2 PC or another fill device. An electronic key distributed through Over-The-Air-Transfer can also be received directly by a fill device.

(2) Loading TEK. Link 16 systems with modernized embedded COMSEC can be loaded with multiple days of TEK. These systems select correct TEK for each day by using the current date information. Service key management policy may restrict the total number of TEK segments that can be loaded, and stored, in a Link 16 system. Normally keys are loaded to support the mission or operational duration. In legacy Link 16 equipment, TEKs must be loaded into the SDU in adjacent pair RAM storage locations. Key management data pre-loaded into the fill device establishes which TEK segment is to be loaded into the correct corresponding SDU RAM location. TEK is loaded into the Link 16 SDU daily. The fill device UAS manages daily key loading. Current fill devices load the current and next day's TEK each time a key is loaded. CT3 compatible fill device software is designed to do this automatically.

(3) CCPD/CPD. Modernized Link 16 systems do not use the CPD and CCPD to manage key use. In legacy, the correct TEK for each day is selected by using the CVLL, network name or default value and current date information. The initialization parameter referred to as the CCPD governs and standardizes which locations are in use on a given day. The CCPD was zero on 1 January 1985 and alternates between zero and one in accordance with Table A 4. (4) Within the terminal initialization load parameters, each of the terminal SDU locations has a CPD associated with it. The terminal will use only the location in which the CPD agrees with the CCPD. The even-numbered locations have the same CPD and the odd-numbered locations have the

opposite CPD. It is important that the terminal operator provide the terminal with information required to establish the correct CCPD. Some system installations require the CCPD to be entered manually from the operator's console. Other systems may require only that the correct date (day, month, and year) be maintained by or entered into the system. A standardized CPD initialization ensures interoperability among universally distributed Link 16 networks. When loaded into the Link 16 system, the same default CPD is set by the initialization data. The current CPD for the network initialization data load must be modified immediately prior to or after KEYMAT loading or reloading.

Table 4. CCPD Determination Values

CCPD Table Non-Leap Years					
2015, 2018,2021, 2023, 2026			2014, 2017, 2019, 2022, 2025		
Month	Day is…		Month	Day is…	
	Odd	Even		Odd	Even
JAN	1	0	JAN	0	1
FEB	0	1	FEB	1	0
MAR	0	1	MAR	1	0
APR	1	0	APR	0	1
MAY	1	0	MAY	0	1
JUN	0	1	JUN	1	0
JUL	0	1	JUL	1	0
AUG	1	0	AUG	0	1
SEP	0	1	SEP	1	0
OCT	0	1	OCT	1	0
NOV	1	0	NOV	0	1
DEC	1	0	DEC	0	1

CCPD Table Leap Years					
2016, 2024			2020,		
Month	Day is…		Month	Day is…	
	Odd	Even		Odd	Even
JAN	0	1	JAN	1	0
FEB	1	0	FEB	0	1
MAR	0	1	MAR	1	0
APR	1	0	APR	0	1
MAY	1	0	MAY	0	1
JUN	0	1	JUN	1	0
JUL	0	1	JUL	1	0
AUG	1	0	AUG	0	1
SEP	0	1	SEP	1	0
OCT	0	1	OCT	1	0
NOV	1	0	NOV	0	1
DEC	1	0	DEC	0	1

(4) Modernized COMSEC System Key Loading. Programmable COMSEC systems such as MIDS JTRS, modernized MIDS LVT modernized JTIDS Class 2 equipment, F-35, and F-22A do not use a location to store keys. These systems use internal key management functionality to select the proper key for the date and the NPG/CVLL. Keys are loaded into these systems by the fill device along with the necessary information for the systems to properly select the keys for use and that information is provided to fill device UAS directly by the user or via a data management system such as DMD or iApp. The SKL and SDS are

currently the only fill devices that can support key loading for these modernized Link 16 COMSEC systems.

(5) Key Loading for legacy Link 16 systems. To ensure that the legacy terminal has the correct CCPD, personnel must ensure that keys are loaded into memory locations that match the CPD assigned by the terminal initialization parameters. The DTD/SKL/SDS UAS manages this function for DS-101 SDUs. For DS-102 protocol key loading, the user must manually set the appropriate switches on the terminal or KCP to select the appropriate SDU RAM storage location to match the automated assignment being made by the DTD/SKL/SDS UAS. The appropriate location information is obtained from the applicable OPTASK LINK message and the crypto period determination table (Table A-4). For Link 16 terminals using a DS-102 type SDU, indications for success of a key load are displayed on the KCP or LCU immediately after each key segment is loaded. For DS-101 SDUs, the DTD/SKL/SDS will display the status of the key load after the load has been completed. The DTD/SKL/SDS also records this information in the key load status log. This log can be reviewed or reset or uploaded to a PC for storage or printing.

2. Key Distribution for Link 16

a. Introduction

(1) Electronic distribution of key is going through a major change. Paper keys are no longer approved. The EKMS is being upgraded to the KMI system. Both of these systems distribute only electronic versions of the required keys. Most Link 16 systems receive the required keys through a fill device connected to the Link 16 equipment fill port. However, some newer Link 16 capable platforms including the F-22A, F -35, and network enabled weapons have special procedures for loading Link 16 keys. The details for these unique key delivery systems will not be provided in this document.

(2) In essence the difference between the EKMS and KMI system is in how the keys are issued to the end user. In the EKMS, the EKMS manager passes the keys to the fill device then that device is issued to the user. In the KMI system, after the user has been issued a fill device, the user retrieves products from the KMI Store-front through network connection to which the user adds the mission data with the iApp and transfers the key with mission data to the fill device. For the EKMS the user has retrieved fill device with keys loaded and loads the mission date from the DMD power station (DMD PS) or ACES system. If encrypted keys (black keys) are provided they are loaded into a DMD PS or ACES system to which the user adds the mission data and loads the combined key and mission data into the fill device. The following sections describe the EKMS and KMI systems in more detail.

b. Key Management Infrastructure

(1) The EKMS and KMI systems both provide the same type of fill process for the Link 16 equipment. KMI is designed to support the delivery of key to all crypto devices in the manner in which they are currently filled in the EKMS. Consequently the fill interface with standard Link 16 equipment is the same whether it is KMI or EKMS providing the key. The remainder of this section addresses how the KMI will support the standard Link 16 systems. The non-standard Link 16 systems are not covered in this document. Examples of standard Link 16 equipment are the MIDS JTRS, the JTIDS Class 2, and MIDS LVT after completion of crypto modernization. Examples of non-standard Link 16 equipment are discussed in paragraph A2, above. The KMI Operating Account (KOA) is similar to the EKMS accounts for the management of authorized users and cryptographic equipment.

(2) Only authorized users may access the KMI Store-front to obtain the cryptographic objects such as keys. The KMI Storefront may only be accessed by users who are authorized by the Controlling Authority (CONAUTH) to receive cryptographic material in accordance with the Account Distribution Profile (ADP). In addition to a properly authorized user at the iApp, only the CONAUTH at a Client Host Only (CHO), and the KMI Operating Account Manager (KOAM) at the MGC can retrieve key from the KMI Storefront.

(3) Only the CONAUTH at the CHO and the KOAM at the MGC can create an ADP and its new key structure from the KMI Storefront. Using the Storefront, the CONAUTH can also modify the ADP for an existing key. These modifications include creation of an ADP for a new key or make required changes to the ADP for an existing key. The key structure created is a uniquely defined series of key(s) that support a cryptonet. And in its ADP the person assigns the KOA that are authorized to participate in the cryptonet. Depending on service policy, the KOAM may or may not modify or create a new ADP. A CONAUTH or KOAM who uses the Storefront to create a new ADP for a key structure becomes the CONAUTH for that key structure.

(4) The information about KMI supplied in this document is for information only. The KMI system has its own architecture. The level of interactions required of the Link 16 is through the fill device and management device such as the iApp, DMD PS, or ACES. The iApp will have the functional capabilities currently in the DMD PS. However, the iApp is considered a KMI-Aware device in the KMI system and is owned by a single KOA. For the Navy and Air Force the iApp will be replacing the DMD PS to provide the mission data for the key loading. The iApp will provide the processing required to connect to the KMI Storefront and unwrap the KMI Over-the-Network Keying (OTNK) wrapped packages and perform any necessary distribution to local element(s) and management functions. For the Army the iApp deployment or upgraded ACES may provide this same service.

(5) Crypto modernized Link 16 equipment requires a separate and new set of keys not associated with the communication channel to initiate/ "boot up" each device. This Key Management Plan (KMP) does not address these equipment keys that each Link 16 equipment needs to function. In particular the Master Key Encryption Key (MKEK) /Unlock key is of this type. In the current design of the Link 16 equipment, the MKEK/Unlock key has the same design as the ECU KEKs. MKEK/Unlock key has to be loaded into the equipment as an unencrypted key. Also, from time to time, it will be necessary to load an ECU KEK into the equipment as unencrypted. The KMI process for loading the MKEK/Unlock keys and other unencrypted keys will be identical to the loading of the unencrypted ECU KEK using the fill device with its TrKEK to provide the unencrypted key to the equipment.

(6) The procedure for loading the unencrypted ECU KEK into the Link 16 equipment uses the capability of the fill device to decrypt keys (Table 5).

(7) The procedure for loading either an encrypted ECU KEK or a TEK into the Link 16 equipment uses the capability of the KMI system to provide encrypted key to the iApp (Table 6). A principal aspect of the use of black key in KMI is that the KOAM is minimally involved. It does not require the KOAM to manage the encrypted TEKs or encrypted ECU KEKs. The major function of the KOAM is to ensure that the security policies are maintained. The Link 16 user uses the iApp to retrieve the encrypted keys from the KMI Storefront. The person then uses the iApp to issue the keys to the fill device. The person then uses the fill device to fill the Link 16 equipment. The steps are as follows:

(8) The KMI is unlike the EKMS. In EKMS a key can be encrypted with a KEK held and then provided to the fill device at the Tier 2 level. In the case of KMI, the normal way a key can be encrypted with another key is through the Storefront. However, an MGC can also encrypt keys and then post them to the Storefront. Link 16 has the capability of using black key. And when KMI can support Link 16, all TEKs shall be delivered to Standard Link 16 equipment as black key. In the case of Emissions Control (EMCON) status all key encryption will have to be anticipated beforehand and held as ROB, since there is no connectivity to the Storefront.

Table 5. Procedure to Load an Unencrypted ECU KEK into Link 16 Equipment

Step	Action	Guidance
1	The KOAM retrieves a TrKEK for the Fill device that is to be used from the KMI Storefront.	If the TrKEK is not authorized or needs to be created, then a CONAUTH will use the CHO to access the KMI Storefront to modify or create the ADP for the TrKEK.
2	At the KOA load the TrKEK into the fill device.	• The KOAM must also associate the TrKEK with the serial number of the fill device. • This action need only be done when a new TrKEK needs to be loaded into the fill device.
3	The KOAM retrieves the ECU KEK that is to be loaded from the KMI Storefront.	The user has to provide the ECU KEK short title to the KOAM. There are plans to allow the iApp to select a designated key and send the key request to the MGC via the Mission Planning Management Support System (MPMSS) Application Program Interface (API).
4	The KOAM encrypts the ECU KEK in the TrKEK that is to be loaded into the fill device.	• The management of the TrKEKs is expected to be done entirely by the KOAM. • The user will provide the ECU KEK identity and the fill device identity to the KOAM. • The user will request the encryption of the ECU KEK for the designated fill device. He will request enough for required ROB. • This action will require the KOAM to translate the fill device serial number into the TrKEK used for the user's fill device and encrypt the key.
5	Use the iApp and request the encrypted ECU KEK to be delivered to the iApp.	None.
6	Issue the encrypted ECU KEK into the fill device	None.
7	Fill the Link 16 equipment with the unencrypted ECU KEK	This action will take place at the operational level.
8	No further action required	At this point the action is complete.

Table 6. Procedure to Load Either an Encrypted ECU KEK or a TEK into Link 16 Equipment

Step	Action	Guidance
1	The user requests the KOAM responsible for his iApp to provide him with an ECU KEK that is to be used with his platform.	• This action does not need to be done often. • An ECU KEK used to encrypt TEKs cannot be used to encrypt ECU KEKs. And an ECU KEK used to encrypt ECU KEKs cannot be used to encrypt TEKs. • The ECU KEK has to be filled into the ECU prior to any corresponding encrypted key being filled.
2	The user requests the KOAM to encrypt a TEK or ECU KEK with the ECU KEK he had previously requested.	None.
3	The user uses the iApp to retrieve the encrypted ECU KEK or TEK.	None.
4	The user uses the iApp to move the encrypted TEK or ECU KEK into the fill device.	None.
5	The user fills the Link 16 equipment with the encrypted TEK or ECU KEK.	This action is accomplished by the operational user.
6	No further action required.	At this point the action is complete.

(9) The request is made to a CONAUTH for a new short title. The CONAUTH can order new key by creating a new cryptonet and establish the accounts that can receive such key through the KMI system using either the CHO or MGC nodes. All compromise resolution has to be done outside the KMI system except the ordering of new keys and changing of who is authorized to receive short titles under his authority. The action to order and control the distribution of keys is done via the KMI Storefront. There are several types of Controlling Authorities. Anyone who orders a new key becomes the CONAUTH for that key. Each KOAM should be the CONAUTH for the TrKEKs used in his account. An official fleet Controlling Authority is responsible for ordering TEK for operational circuits. Any operational command should have this authority. Any Link 16 user should be responsible for ensuring that his TEKs are encrypted with a KEK designated for his keys. However, the user may not have a connection into the KMI system to become a CONAUTH, in this case, the user requests of the KOAM to request an ECU KEK for his/her equipment. And for training purposes, the local command may request the KOAM to become the CONAUTH for TEKs to be used by the platforms under his command.

(10) Request is made for an NSA encrypted key to be delivered via the Defense Carrier Service with an ECU KEK already in the KMI system. Normally, NSA does not want any key to be delivered in physical form. However, Link 16 is in operation in many countries that do not have the capability of handling electronic key. NSA will have to make a decision as to how these countries will receive key. It could be through physical media or by the use of transporting fill devices. The order still goes through the KMI system.

c. Electronic Key Management System

(1) Description. The EKMS is a key management, COMSEC material distribution and logistics support system consisting of interoperable Service and Defense agency key management systems. NSA established EKMS to meet multiple objectives, including supplying electronic keys to COMSEC devices in a secure and timely manner and providing COMSEC account managers with an automated system capable of ordering, generating, producing, distributing, storing, securing, accounting, and controlling access. Other EKMS features include automated auditing capabilities to monitor and record security-relevant events, account registration, and extensive system and operator privilege management techniques to provide flexible access control to sensitive key, data, and functions within the system. Common EKMS components and standards will facilitate interoperability and commonality among the Services.

(2) Purpose. The goal of EKMS implementation is to reduce the potential for KEYMAT exploitation by reducing human access to KEYMAT during distribution.

(3) Functional Description. EKMS consists of the four tiers described below.

(a) Tier 0. The National Security Agency Central Facilities (NSACF) provides a broad range of capabilities to the Department of Defense and other government agencies. These facilities comprise the EKMS Tier 0 and include the facilities located at Fort Meade (CFFM) and Finksburg (CFFB), Maryland. CFFM will continue to produce the modern (FIREFLY and other electronic short titles) key.

1. NSACF Functions:

a Seed conversion and rekey.

b Compromise recovery and management of certain key material.

c. Physical and electronic key order processing.

d. Electronic key generation and distribution.

e. Conversion of existing key to EKMS (ensuring backward compatibility is retained).

2. Communications. The NSACF communicates with other EKMS elements through a variety of media, communication devices, and networks including direct distance protected data communication access (Secure Terminal Equipment (STE)) or dedicated link access (Omni, Omega, and KG-84/KIV-7HS/HAIPE). Direct communication between tiers is not always available. During transition to the full electronic key the CD disk will be supported between EKMS Tier 2 and Tier 3. Once fully operational, a Transmission Control Protocol/Internet Protocol (TCP/IP)-based message server will be the primary means of communication with the NSACF via KMI. This service will permit KMI elements to store messages that include the electronic key for later retrieval by other elements.

(b) Tier 1. Each Service maintains a central office of record (COR) that performs basic key and COMSEC management functions, including key ordering, production, distribution, and inventory control. The EKMS Common Tier 1 serves as the distribution point for the Service CORs.

(c) Tier 2. Tier 2 comprises the local account holders at user activities and consists of a Service-supplied or agency-supplied LMD and an NSA-supplied KP. The LMD is a Service-supplied or agency-supplied commercial off-the-shelf (COTS) PC. NSA-supplied local communications security management software (LCMS) was developed to replace Service-unique automated software. LCMS is the software that provides COMSEC account managers with the capability to electronically generate the local COMSEC key using the KP; order COMSEC material; distribute, inventory, and destroy KEYMAT; and perform other COMSEC management functions. UAS is being developed to provide key management for newer COMSEC equipment and weapons systems and will serve as the operator interface for LCMS.

1. Software. LCMS provides the interface between the LMD and the KP and tools for COMSEC management. Specialized application programs have been developed by several departments and agencies that overlay the LCMS and provide tailored human-machine interface.

2. Platform. The LMD operates the Santa Cruz Operations (SCO 5.0) operating system and hosts LCMS. When the LMD and KP are used together, the account custodian/manager is able to order and account for all forms of COMSEC key material, store the key in encrypted form, perform key generation and automatic key distribution, perform COMSEC material accounting functions, and communicate directly with other EKMS elements.

3. KP. The KP performs cryptographic functions, including encryption and decryption, key generation, and electronic signature operations. The KP is capable of secure field generation of a traditional key. A locally generated key can be employed in cryptonet communications, TRANSEC applications, point-to-point circuits, and virtually anywhere that paper-based keys are used today. Electronic keys can be downloaded directly to a fill device for further transfer or fill to the ECU.

(d) Tier 3 Fill Device. The Usable fill devices for Link 16 are an NSA-certified, portable handheld device capable of securely receiving, storing, and transferring data between compatible cryptographic and communications equipment. They are capable of storing 1,000 symmetric keys; they maintain an automatic internal audit trail of all security-relevant events that can be uploaded to the LMD/KP; they encrypt the keys for storage; and they are programmable. The fill device is capable of keying multiple COMSEC devices and is compatible with such COMSEC equipment as single-channel ground and airborne radio system radios, VINSON, KG-84, and others that are keyed by common fill devices (CFDs). The fill device is designed to be fully compatible with COMSEC equipment meeting DS-101 and benign fill standards.

1. Tier 3 AN/PYQ-10(C) (SKL). The SKL is backward compatible with existing ECUs and forward compatible with future equipment. The SKL is a handheld digital computer running a Windows CE Net operating system hosting the core library and SKL UAS programs that interface with the LCMS workstations, DMD software, and ECUs on the battlefield. The SKL provides for the receipt, display, transmission, preparation, storage, and accountability of key material and signal operating instructions information. The SKL has been ruggedized to withstand battlefield conditions. The SKL is a controlled cryptographic item (CCI) because of the KOV-21 information security card imbedded in it. When classified database information resides in the SKL, the SKL takes on the classification of the data. The SKL provides the same functionality as and is backwards compatible with the CT3 UAS that resides in the AN/CYZ-10 (DTD).

2. Tier 3 KIK-20 (SDS). The SDS is a portable handheld device capable of securely receiving, storing, and transferring electronic data between compatible communications equipment. The SDS provides the same functionality as and is backwards compatible with the CT3 UAS that resides in the AN/CYZ-10 (DTD).

(e) Key Distribution. Paper tape key distribution will no longer be available. Users that do not have electronic distribution capability will have to obtain keys via physical transport of fill devices. For EKMS, the connection between Tier 2 and Tier 3 can be remote using various secure communication systems. The key may be loaded into the fill device directly by connecting the fill device to the LMD/KP or KMI Advanced Key Processor (AKP), remotely by

loading the key into a local fill device and then transferring the keys and database to another fill device via a secure communication connection to a remote site, and remotely by loading the key into a local fill device and then sending the keys to a remote site via the secure transfer where the key is collected in a remote fill device at the user site.

(f) EKMS Key Request Process. Much of the TEK generation will occur at Tier 0 due to the requirement for the need to distribute the key to allies. TEK for US ONLY may be generated at Tier 1 or Tier 2. ECU encrypted key is encrypted at Tier 2 using locally available UAS. Each Service has a policy on where the KEK keys for the encryption are to be generated and managed.

d. Key Ordering Parameters for KMI and EKMS

(1) Parameters. The following subparagraphs describe typical parameters for ordering operational keys. It is expected that each command would order its own keys. Table A-5 describes the keys that each command may desire to order.

Table 7. Operational Link 16 Key Allocation

	Worldwide Emergency	**Joint Theater**	**Allied**
DHS	Note 1	Note 8	Note 15
NORAD	Note 1	Note 6	Note 13
USCENTCOM	Note 1	Note 4	Note 11
USEUCOM	Note 1	Note 2	Note 9
USNORTHCOM	Note 1	Note 7	Note 14
USPACOM	Note 1	Note 3	Note 10
USSOUTHCOM	Note 1	Note 5	Note 12
USSTRATCOM	Note 1		

Note 1: This allied key is to be ordered by the CONAUTH designated by USSTRATCOM.
Note 2: These US keys are to be ordered by the CONAUTH designated by USEUCOM.
Note 3: These US keys are to be ordered by the CONAUTH designated by USPACOM.
Note 4: These US keys are to be ordered by the CONAUTH designated by USCENTCOM.
Note 5: These US keys are to be ordered by the CONAUTH designated by USSOUTHCOM.
Note 6: These allied keys are to be ordered by the CONAUTH designated by NORAD.
Note 7: These allied keys are to be ordered by the CONAUTH designated by USNORTHCOM.
Note 8: These allied keys are to be ordered by the CONAUTH designated by DHS.
Note 9: These allied keys are to be ordered by the CONAUTH designated by USEUCOM.
Note 10: These allied keys are to be ordered by the CONAUTH designated by USPACOM.
Note 11: These allied keys are to be ordered by the CONAUTH designated by USCENTCOM.
Note 12: These allied keys are to be ordered by the CONAUTH designated by USSOUTHCOM.
Note 13: These allied keys are to be ordered by the CONAUTH designated by NORAD.
Note 14: These allied keys are to be ordered by the CONAUTH designated by USNORTHCOM.
Note 15: These allied keys are to be ordered by the CONAUTH designated by DHS.

(a) Equipment Type. Legacy Link 16 uses a variety of SDUs. EKMS recognizes only the KGV-8, KGV-8B and modernized Link16 equipment types. The Link 16 system only uses the TEK usage type of key for transmission and communication security. These keys can be filled as unencrypted or and encrypted keys. The generation, management, and delivery of these keys to the Link 16 equipment are provided for in the processes of the KMI, EKMS LMD with the KMI Common User Application Software (CUAS), the iApp, DMD PS, or ACES software applications, and fill devices. All of the Link 16 equipment can use the Standard TEK type and the Accordion 1.3 KEK type of keys. However, the modernized Link 16 can use keys of Suite A and Suite B design which are described in the NSA document "Key Specification for the Link-16 Family of Equipments."

(b) Desired Order Type. The desired order type cues EKMS or KMI to create the short title.

(c) KMI or EKMS Account ID. Only Tier 0 can meet the requirements for generating Allied key; therefore, the ID for key generation will normally be 880091 (NSACF). If the key is generated locally by an EKMS Tier 2, by an EKMS Tier 1, or by the Storefront entity, the appropriate ID shall be used.

(d) Key Use. The only key of interest for the joint community is the TEK. ECU KEK and TrKEK that are generated by the Services, or locally, may also be considered.

(e) Key Purpose. Typically, this field will be "Operational." Other types of keys (training, test, or maintenance) may be ordered as needed by using the parameters of this enclosure.

(f) Handling Restrictions. Keys are to be handled in accordance with CMS doctrine.

(g) Net Size. Cryptographic nets should be as small as operationally practical.

(h) Crypto Period. Link 16 KEYMAT for a daily key has a cryptographic period beginning at the beginning of the first minute of the day defined by UTC and ending at the end of the last minute of the day as define by UTC. Although a seven day key is designed as a capability of the Link 16 equipment, it is not used without explicit coordination and a joint service agreement. Current infrastructure is not designed to support its use.

(i) Segments/Edition. Daily keys are designed around the concept that the segment number and day of the month are the same. Thirty-one segments per edition are used to reflect this correspondence.

(j) Accounting Legend Code. Since the operational key is reportable to the COR, the Accounting Legend Code (ALC) number is 6. Locally accountable training, test, or maintenance keys are designated ALC-7.

(k) Classification. Any key used for Link 16 over-the-air operations must be at least SECRET. Maintenance keys may be UNCLASSIFIED For Official Use Only (FOUO).

(l) Supersession Rate. Link 16 key Editions shall have a monthly supersession.

(m) Distribution Control. An entry of "Implicit" indicates that the key may be copied IAW the directions of the CONAUTH. The CONAUTH must add any new accounts to the distribution profile (see subparagraph 4a(20)) to ensure that the account's ROB is adequately supported by the Tier 0 key generating account. For non-operational keys with no standing order, copies may be adequate.

(n) Auth ID. [List all CONAUTHs.] This would be the combatant command or JCMO ID for the operational key. The non-operational key may specify a different CONAUTH.

(o) Release. [Restrictions on release.] For example, NOFORN, USA/CAN/GBR ONLY or FVEY.

(p) In-Place Date. This is the date the user requests for KEYMAT delivery.

(q) Effective Date. [Date the first key segment is effective.] No entry is currently required. The CONAUTH can establish this at a later time.

(r) Standing Order. This field indicates whether the key will be produced on a continuing basis to meet the ROB requirement of all receiving accounts.

(s) Edition Information. This is the number of editions to be generated at one time. One edition is generally adequate. The maximum ROB of all the accounts to receive the key will dictate the actual number of editions produced. If there is no standing order for the key, the ordering agent must determine the number of editions to be generated as a one-time production.

(t) Distribution Profile. [List intended recipient(s) EKMS ID(s).] At least one account must be provided. The CONAUTH may add additional accounts as needed.

(u) [NATIONALITY]. This field indicates whether the key is US or Allied. Although "NATIONALITY" is included here as a placeholder, the title of this field is currently undetermined.

(2) Examples of Typical Parameters

(a) Equipment Type: KGV-8 or LINK16CM

(b) Desired Order Type: Assign

(c) KMI or EKMS- ID: 880091 (KMI or EKMS - ID of the generating element; Tier 0)

(d) Key Use: TEK

(e) Key Purpose: Operational

(f) Handling Restrictions: No restrictions

(g) Net Size: 40

(h) Crypto period: Daily

(i) Segments/Edition: 31

(j) ALC: ALC-6

(k) Classification: SECRET

(l) Supersession Rate: Monthly

(m) Distribution Control: Implicit

(n) Auth ID: (COCOM or JCMO ID)

(o) Release: NOFORN, USA/CAN/GBR, FVEY

(p) In-Place Date: (Date the key is required to be in place at the destination; when ordering the joint operational key, date must match the Defense Courier Service delivery date.)

(q) Effective Date: (Date the first key segment is effective.)

(r) Standing Order: Y

(s) Edition Info: 1

(t) Distribution Profile: (combatant command or JCMO ID)

(u) U.S. or Allied (See Table A-5.)

(3) Joint Operational Keys. Short titles for the keys described in Table A-5 are dynamic, and not currently available. They will be provided in future revisions of this manual as they are developed. The baseline CONAUTH responsibilities are described in reference e, Committee on National Security Systems Instruction (CNSSI) 4006. CONAUTH responsibilities are detailed in the corresponding Service manual of the supported Service.

3. Joint Key Management Plan Procedures

a. Key Management Responsibilities

(1) Combatant Commanders. Combatant commanders will:

(a) Direct CCMD assigned JICO to provide network design criteria to their Service Network Design Facility (NDF) to include COMSEC key structure. These criteria will be in the form of specifying details such as cryptonet requirements, CVM, or PVM usage.

(b) Direct CCMD assigned JICO to prepare and distribute OPTASK LINK message preparation guidance and specific key management instructions to include current CVLL assignments.

(c) Notify CONAUTHs of joint theater key requirements.

(d) Implement standing orders and/or dynamic ordering procedures to support anticipated robust network structures.

(e) Order short titles for joint and combined in-theater requirements.

(f) Anticipate and fund requirements to enable electronic key distribution to coalition partners.

(g) Notify Service Acquisition Agencies, Coalition Partners, and US country teams of US requirement for US COMSEC custodians to meet the needs for FMS accounts.

(2) Network Design Facilities. Service NDFs develop networks for operations, tests, exercises, experiments, and training. Cryptonets must include only the participants that have a need to see data protected by the network. This is managed by maintaining the pairing of NPG assignments and CVLLs.

(3) KOAM and EKMS Managers. COMSEC Account Managers (CAM) develop procedures to support delivery of key to Link 16 equipment.

(a) Normal Functions. Each Service has instructions concerning the CAM duties including the requirement to maintain a COMSEC inventory and Link 16 ROB adequate to support the command operational mission. Each Service is responsible for ordering short titles for intra-Service operations and testing.

(b) COMSEC Support. The support of Link 16 Network keying requirements levies additional responsibilities on the CAM. In addition to the key distribution functions, there are Service-specific CUAS programs on the EKMS Tier 2 LMD used to support the CT3 system on the fill device. The CAM will need to operate the CUAS to support the Link 16 system. In some cases, the CAM will be responsible for loading all platform and equipment data as well as loading the keys into the fill device. The CUAS will support Link 16 operations and other cryptographic material by providing the CAM with a method of identifying and creating all the management information required by the fill device. The CUAS is capable of requesting key and key encryption with an ECU KEK and providing that information to a DMD PS or a fill device. The CUAS is also capable of requesting a key and encrypting it in a specified fill device TrKEK for key transfer when the ECU must receive an unencrypted key. If the user has a workstation and software, the user may provide all data on a floppy disk or on a paper sheet. In that case, the COMSEC account manager needs only to assist in loading the fill device or ECU KEKs and operate CUAS to provide the data and encrypted keys on a floppy or download this information into the fill device. The user on a workstation or DMD PS is responsible for ensuring the keys are correctly assigned to the ECU.

(c) Audit Log Maintenance. Audit logs for programmable COMSEC Link 16 systems are normally accessible only by the Original Equipment Manufacturer (OEM). Maintenance of the fill device audit log is directed by Service instructions and will be followed by users. The local commander is responsible for implementing the procedures and doctrine specified for the fill device as developed by the various Services. The CAM is responsible for ensuring that proper procedures are carried out regarding uploading, viewing, and resetting of the fill device audit log. Additionally, the CAM is responsible for instructing the user in the user's responsibilities.

(4) Users

(a) Loading Keys. The user is responsible for loading the correct keys for the mission into the SDU. The fill device will assist the user in the selection of the correct segments for key loading. In order to comply with IAD MD 10, only encrypted TEK shall be loaded into a Link 16 system. Either encrypted or unencrypted ECU KEK may be loaded into Link 16 systems. TEKs may be encrypted by NSA or locally encrypted by the COMSEC account LMD/KP or

KMI MGC workstation. The intent is to meet IAD MD10 by protecting the TEK from its original generation point all the way to the ECU, with unencrypted TEK never being accessible outside of the LMD/KP or MGC.

(b) Zeroizing Equipment. All Link 16 SDUs, including the programmable COMSEC systems, will zeroize all unencrypted TEK upon removal of power. Link 16 terminal operators must actively zeroize the SDU if the unit is likely to fall into enemy hands. Some aircraft provide a switch that will zeroize all equipment including Link 16, while in some systems the operator of the host system must send an initiate command to zeroize the Link 16 equipment. The fill device can also be used to zeroize the TEK keys and in the legacy systems this is the only way to zeroize the ECU KEK keys. During normal operation, the ECU KEKs need to be zeroized only if the SDU is to be stored for more than a month or shipped through commercial shipping.

(c) Monitoring Alarms. The SDU alarm sensors monitor internal operations and perform self-tests on the alarm circuitry. Alarm conditions can be caused by loss of power sources, invalid key transfers to the SDU, time slot number errors, and problems with physical parts within the SDU. If an alarm condition occurs, it is reported to the host terminal. The SDU then performs a series of internal checks and attempts to restore the keys in use. If the internal test failures persist, the SDU will not operate. It is the user's responsibility, upon observing an alarm condition, to evaluate the condition, determine what action is necessary to ensure security of the communication data, and take corrective action where appropriate. SDUs for which alarms cannot be removed should be evaluated for repair. The terminal CRYPTO HOLD battery, not the SDU, causes the most common problems. Proper terminal battery care will minimize the occurrence of SDU alarms.

(d) Maintaining Audit Log. Service instructions establish requirements and procedures for fill device audit log maintenance. At their discretion, local commanders may provide additional guidance to the COMSEC account manager. Users are responsible for complying with all applicable guidance.

(e) Preparing Data for the Fill Device. The software in the fill device requires that platform and equipment data be programmed into the fill device in addition to the key. The user will be required to either manually enter this platform and equipment data or retrieve the data from a workstation. An operator can create the platform and equipment information by using the ACES system, the iApp or the DMD PS. If the CUAS provides the encrypted key to the ACES, iApp, or DMD PS, the operator can also assign the key to the appropriate ECU. These systems deal with encrypted key only and can download the platform, equipment, and assignment data. For the SKL to have the information needed to fill the Link 16 equipment requires the unencrypted key in the SKL be tied to information of where and how the key is to be used in

the Link 16 equipment. There are three strategies to tie them together. The first strategy is as follows: The first is to load the information into the SKL in much the same way as above for the encrypted keys. Then the fill device must receive all unencrypted key from EKMS or KMI in key-needed mode. The second strategy is as follows: Let the fill device receive all unencrypted key from EKMS or KMI. Then use the DMD PS, iApp, or ACES to load the other information. Both of these strategies require that the DS-100 short title information be exactly the same. The third strategy is as follows: Let the fill device receive all unencrypted key from EKMS or KMI. Then use the capabilities of the SKL to have the user build the support information through the man machine interface.

(f) Monitoring Cryptographic Material Access. Access control for KEYMAT and COMSEC equipment is defined in the applicable COMSEC and EKMS doctrine for each Service. Normally, when the Link 16 SDU has a KEK installed, the equipment is handled locally as unclassified CCI. If the equipment is to be put in long term storage or to be shipped every effort must be made to zeroize the KEK. If it is not possible to zeroize the KEK, then it is to be handled as SECRET. For crypto upgraded terminals, it is good COMSEC practice that the equipment should have all the KEK and TEK erased/zeroized if the equipment is not in use and is stored for a month or more or is to be transported to another location. Link 16 terminals are considered high-value items. Protection afforded to the Link 16 terminal is adequate for the SDU that is associated with it. No special clearance is required to observe filling of any Link 16 SDU by an electronic fill device. Access to a fill device, which is also a CCI device, is covered in each Service EKMS or COMSEC doctrine. Viewing of a fill device or fill process, by personnel without COMSEC training or user status is permitted, except when loading a key marked “CRYPTO” in paper form.

(g) Monitoring Link 16 System Access. Keys are not extractable from any of the Link 16 SDUs discussed in this document. Personnel possessing clearances to the level of the traffic transmitted or received are permitted access to the areas operating a Link 16 terminal. CMS user status is not required unless the key is exposed. Anyone may observe the Link 16 equipment with or without the SDU being visible. Modernized Link 16 equipment is to be handled as CCI. Link 16 SDUs for all operational units are CCIs and should be handled IAW current CCI doctrine. All Link 16 systems are considered CCIs. Special handling doctrine should be utilized to accommodate the large equipment.

(h) Accounting. Link 16 key accounting is accomplished via the EKMS or KMI accounting system and will comply with Service COMSEC doctrine and EKMS UAS capabilities or KMI criteria.

b. Key Generation

(1) TEK. Joint TEK will normally be generated at Tier 0, by KMI, or at EKMS Tier 1. TEK may be generated at the EKMS Tier 2 or MGC level in special circumstances. Each Service may have the keys used for their operations generated with EKMS or KMI.

(2) ECU KEK. When the generation of ECU KEKs is required, they should be generated at the lowest level of EKMS or KMI facilities that can provide the KEK to the user that needs it. Common ECU KEKs are required for locations in which there is shared fill device usage, even if it is only for emergency backup. For example, all elements of a USN battle group will have the same ECU KEKs, allowing any fill device with Link 16 ECU encrypted keys to load any Link 16 SDU in that battle group.

(3) Fill Device KEK. Fill device KEKs (TrKEKs) are part of the EKMS and KMI concept of operations.

c. Key Distribution. Table A-6 details the nominal operational requirements for a key to support a combined task force. Short titles listed are only examples. At a minimum, two coalition-releasable and two US-only cryptographic short titles are required. The equipment addressed by this document has specifications that require that at least 1000 keys can be loaded into the equipment. The 1000 keys can be of any mix of TEKs, KEKs, and system keys. Programmable COMSEC systems may load many short titles to support different missions. Service doctrine may limit the number of editions or segments of each short title that may be loaded into an SDU. The contingency key is included to support emergent COMSEC interoperability requirements. Each Service is responsible for ordering short titles for intra-Service operations and testing.

Table 8. Nominal Combined Force COMSEC Requirements

Link 16 Key Type	Users	Purpose
MSEC	All US Forces Users	US Force Tactical Data
MSEC	Specified US Forces Users	US Air-to-Air
MSEC	Specified Coalition Users	Coalition Air-to-Air
MSEC[1]	All Users	Coalition Tactical Data
TSEC	All Users	Network Synchronization
TSEC or MSEC	All Users	Emergency Contingency

[1] One short title may be used to satisfy common TSEC and MSEC requirements.

(1) Requesting Key. The required key must be requested by the EKMS Tier 2 COMSEC account supporting the user from the EKMS Tier 0 or Tier 1 facilities. To minimize risk of compromise and vulnerability to exploitation, ECU encrypted keys, both TEK and KEK, shall be used wherever feasible. A similar process is used for requesting key from KMI.

(2) USMC Key Management. USMC Legacy Link 16 terminals use unencrypted TEKs and KEKs in electronic form. To request keys, the COMSEC Manager, per EKMS 1B, will submit a Modification of Allowance through his/her chain of command to the appropriate Marine Forces Command. The CONAUTH will be courtesy copied on a final endorsed message; generated by NSA; and then transferred electronically to user accounts by the NSA-managed National Distribution Authority. Encrypted TEKs are loaded into fill devices using black key management support software. Local COMSEC account managers submit key requests through the responsible CONAUTH.

(3) Receiving Key

(a) ECU KEK. Tier 2 distribution points may receive their ECU KEK from Tier 0/1 or generate KEK for distribution to their user accounts. User COMSEC accounts may receive Link 16 KEK in their Tier 2 LMD/KP directly from Tier 1 or from their serving EKMS Tier 2 distribution point for further issue to a fill device for loading into an ECU.

(b) TEK. User COMSEC accounts may receive TEK in their Tier 2 LMD/KPs from either Tier 1 or Tier 0 or their serving EKMS Tier 2 distribution point. TEKs may be encrypted at Tier 2 using a KEK obtained from a Tier 1 facility (or generated locally) upon request from a Tier 2 UAS (e.g., CUAS) and the resulting encrypted TEK distributed by the Tier 2 UAS to the fill device.

d. Key Storage

(1) SDU. All Link 16 SDUs are capable of storing unencrypted keys. Programmable COMSEC systems can store 1000, or more, keys of all types. All keys stored in the SDU are non-extractable.

(a) RAM Storage. The network selected for terminal initialization controls the actual CVLLs used. Once a network has been selected (or constructed by an NDF based on operational requirements), the Short titles are promulgated in the OPTASK LINK based on the usage defined in the Network Description Document COMSEC Cross-Reference Table. Planners use this table to determine the number of CVLLs and, thus, the number of separate keys required to operate the network as well as the CVLLs for each key.

(b) Programmable SDU Storage. Programmable Link 16 SDUs do not use a location mapping paradigm. Keys are assigned to a specific CVLL prior to loading into the SDU. The Link 16 terminal manages the use and rollover of all of the keys loaded.

(2) Fill devices. The fill devices can store at least 1,000 unencrypted TEKs and their associated key tags. ECU encrypted keys are larger than unencrypted keys; consequently, fewer encrypted keys can be stored. Stored

keys can be secured by removing the crypto ignition key (CIK) from the device. With its CIK removed, the fill device becomes an UNCLASSIFIED CCI device. Stored keys can be selectively deleted or zeroized. The fill device must be zeroized to remove all keys and downgrade the fill device to UNCLASSIFIED CCI.

e. Key Loading. Single point keying (where several cryptographic devices using the DS-101 protocol can be keyed at the same time over a fill bus) has been implemented in some Link 16 platforms. A bus (STATION) address is used during DS-101 key loading to direct keys to the correct terminal SDU. The management of station addresses for bussed SDUs is the responsibility of each Service platform program office (e.g., NAVAIR PMA-265 for the F/A-18). KMI and EKMS support single point keying.

f. Crypto Periods

(1) KEK. The crypto period for each Link 16 ECU KEK Segment to encrypt TEKs is one calendar month commencing on the first day of the month at exactly one before 0001 UTC. The special ECU KEKs used to encrypt other ECU KEKs is one calendar year. Because ECU KEKs are not used directly for communication, there is no urgency in getting the ECU KEK loaded when it becomes effective. The ECU KEK needs to be loaded before the next set of black keys using the ECU KEK are loaded.

(2) TEK. The crypto period for each Link 16 TEK is one day and commences exactly at the beginning of the first minute of the day defined by UTC." In general, Link 16 keys are loaded prior to the day they are effective to support automatic rollover. With good management, there is no panic to get the keys loaded for next day operations because Link 16 keys are authorized to be loaded prior to their effective date.

(3) CPD Initialization. For legacy Link 16 equipment as applicable, even-numbered RAM locations shall be initialized to the same CPD (normally 0) and the odd locations shall have the opposite CPD (normally 1). Modernized Link 16 equipment does not use CPDs.

(4) Crypto Period Extension. The Link 16 design does not permit operator-initiated extension of the key crypto period. .The cryptographic period for Link 16 is 24 hours, normally commencing at the beginning of the first minute of the day defined by UTC. Explicit coordination and a joint Service agreement are required to use a seven-day crypto period and will be addressed in a separate addendum to this plan when the engineering is accomplished to use this capability.

g. Compromise Procedures. COMSEC incidents are reported in accordance with reference f, CNSSI 4003, "Reporting and Evaluating COMSEC Incidents" and its Service implementers.

(1) Unencrypted TEK Compromise. If an unencrypted TEK is compromised, the encrypted copy of the same TEK is also compromised. Compromise recovery strategy is to supersede the compromised TEK edition and use the next sequential TEK edition. If TEK recovery requires a KEK change, the appropriate KEK segment used to encrypt/decrypt the encrypted TEK must be superseded, and the next KEK segment shall be used. The compromise of a TEK does not automatically compromise KEKs.

(2) Encrypted Key Compromise. Loss of an encrypted TEK or encrypted KEK is not a compromise. A physically lost key shall be replaced with an identical key.

(3) Unencrypted KEK Compromise. If an unencrypted KEK is compromised, all keys encrypted with that KEK are also compromised. The recovery procedure for a compromised KEK segment is to supersede that segment and all editions of keys encrypted by that KEK and implement the next KEK segment and corresponding key edition encrypted by that KEK. Note that when a KEK is compromised, that each and every TEK encrypted by that KEK are also compromised. Even if the TEK had been received by some other means, it is still compromised. The recovery procedure for a compromised KEK edition is to supersede all key editions encrypted by that KEK and implement the next KEK edition and corresponding key editions encrypted by that KEK. If no uncompromised KEK editions and associated encrypted keys are available, new KEKs and TEKs must be requested from the EKMS Tier 1, Tier 2 facility, KMI, or NSA.

h. Operational Tasking Data Link . The formatted message for OPTASK LINK defined by MIL STD-6040 is used to provide detailed instruction regarding the tactical data link operations. The OPTASK LINK contains COMSEC key identification, link operating frequencies, channelization, and initialization plans. The OPTASK LINK is used by terminal platforms to plan and conduct joint tactical communications for a designated period. Instructions for the preparation and loading of the COMSEC/CRYPTO keys required for link operation are included in the Link 16 portion. Each OPTASK LINK message contains network start times, which specify the effective period of operation for the tactical data links. The cryptographic data section of the OPTASK LINK message specifies unique COMSEC requirements. It relates COMSEC short titles to CVLL. For legacy Link 16 it generally provides the memory locations for the CVLLs as amplifying information. Also for legacy Link 16, it may have amplifying information for what the CCPD value should be on the first day of the use of the network.

(INTENTIONALLY BLANK)

ENCLOSURE B

LINK 16 COMSEC ENTITIES CONTACTS LIST

Agency	Message Address	Web Address
SPAWARSYSCEN Pacific 58120 53560 Hull St San Diego, CA 92152-5001	SPAWARSYSCEN PACIFIC CA//58120//	
Director, National Security Agency 9800 Savage Rd Ft. George G. Meade, MD 20755-6000	DIRNSA FT GEORGE G MEADE MD//I824/I541//	
AFLCMC /HNCDX 304 North Frank Luke San Antonio, TX 78236-1851	DIR TIER1SAN ANTONIO TX	https://lackland.eis.aetc.af.mil/cpsg/default.aspx
AFLCMC /HNCDX 304 North Frank Luke San Antonio, TX 78236-1851	HQ CPSD SAN ANTONIO TX//	https://lackland.eis.aetc.af.mil/cpsg/directorates/mi/default.aspx
Joint COMSEC Management Office 901 SAC Blvd STE 2B9 Offutt AFB, NE 68113	Message Address: JCMO OFFUTT AFB NE	https://vela.stratcom.smil.mil/restrict/jcmo
Naval COMSEC Material System, 1560 Colorado Ave Camp Springs, MD 20707-6108	NCMS WASHINGTON DC//N3//	http://www.cyberfor.navy.mil/
Joint Interoperability Test Command Ft. Huachuca, AZ 85635	CDRJITC FT HUACHUCA AZ//JTEB//	
US ARMY CECOM LCMC CSLA 2133 Cushing St, STE 3600 Fort Huachuca, AZ 85613-7041	DIRUSACSLA FT HUACHUCA AZ//AMSEL-LCA-KEY	usarmy.huachuca.cecom.list.csla-tier-5a8240-key@mail.smil.mil
CYSS/CYS 203 W. Losey St Rm. 2200 Scott AFB, IL 62225-5222	HQ AFNIC SCOTT AFB IL//ECAP//	
USPACOM J63 Bldg. 700 Camp Smith, HI 96861-4029	HQ USPACOM HONOLULU HI//J63//	

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. CJCSM 6120.01 Series, "Joint Multi-Tactical Data Link (TDL) Operating Procedures"

b. CJCSM 6510.01 Series, "Cyber Incident Handling Program"

c. NAG-45A, August 2001, "Operational Security Doctrine for Joint Tactical Information Distribution Systems (JTIDS)"

d. "Operational Security Doctrine for the Multifunctional Information Distribution Systems (MIDS)," December 2008.e.d. Operational Security Doctrine for the Multifunctional Information Distribution System, Joint Tactical Radio System (MIDS JTRS), March 2012

e. Committee on National Security Systems Instruction (CNSSI) 4006, 17 April 2012

f. Committee on National Security Systems Instruction (CNSSI) 4003, 27 May 2014

g. Information Assurance Directorate (IAD), IAD Management Directorate 10, Revised 15 July 2011

h. Committee on National Security Systems, Controlling Authorities for Traditional Communications Security (COMSEC) Keying Material, 17 April 2012

i. Key Specification for the Link-16 Family of Equipments, Rev.: 12, 15 January 2014

(INTENTIONALLY BLANK)

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

ACES	Automated Communications Engineering Software
ADAM-Cell	Air Defense and Airspace Management (ADAM) Cell
ADP	Account Distribution Profile
ADTOC	Air-Defense-Tactical-Operations-Center
AFNIC	Air Force Network Integration Center
AKP	Advanced Key Processor
ALC	Accounting Legend Code
AMF	Airborne and Maritime/Fixed Station
AOR	Area of Responsibility
API	Application Programming Interface
ASTOR	Airborne Stand-Off Radar System
AWACS	Airborne Warning and Control System
BCS-M	Battle Control System Mobile
C2	Command and Control
C2P	Command and Control Processor
CAC2S	Common Aviation Command and Control System
CAN	Canada
CAM	COMSEC Account Managers
CANTPRO	Can't Process
CCEB	Combined Communications Electronics Board (5 eyes)
CCI	Controlled Cryptographic Item
CCPD	Current Cryptographic Period Designator
CCSD	Cryptologic and Cyber Systems Division
CDH	Communications Security/Transmission Security Integrated Circuit Data Standard 101 Hybrid
CECOM	Communications-Electronics Command
CFD	Common Fill Device
CFFB	Central Facility Finksburg
CFFM	Central Facility Fort Meade
CG	Guided Missile Cruiser
CHO	Client Host Only (KMI)
CIK	Crypto Ignition Key
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CKG	Combat Key Generator
CMCS	COMSEC Material Control System
CMN	Concurrent Multi-Netting

CMS	Communications Security Material System
CNSSI	Committee on National Security Systems Instruction
COCOM	Combatant Commander
COMSEC	Communications Security
CONAUTH	Controlling Authority
COR	Central Office of Record
COTS	Commercial off the Shelf
CPD	Cryptographic Period Designator
Cryptonet	Cryptographic Network
CSLA	Communications Security Logistics Activity
CSN	Central Services Node (KMI)
CSP	Common Signal Processor
CSS	Crypto Sub System
CT3	Common Tier 3
CTIC	Communications Security/Transmission Security Integrated Circuit
CUAS	Common User Application Software
CVLL	Cryptographic Variable Logic Label
CVM	Common Variable Mode
CVN	Aircraft Carrier, Nuclear Powered
DCS	Defense Carrier Service
DDG	Guided Missile Destroyer
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMD	Data Management Device
DOC	Delivery Only Client (KMI)
DoD	Department of Defense
DS	Data Standard
DTD	Data Transfer Device
ECU	End Cryptographic Unit
EEPROM	Electronic Erasable Programmable Read-only Memory
EKMS	Electronic Key Management System
EMD	Engineering and Manufacturing Development
FDL	Fighter Data Link
FOC	Full Operational Capability
FOUO	For Official Use Only
FVEY	Five Eyes
GBR	Great Britain
GTACS	Ground Theater Air Control System

HAVCO	Have Complied
HPA	High Power Amplifier
IAD	Information Assurance Directive
iApp	KMI Intermediary Application
IEEE	Institute of Electrical and Electronics Engineers
IJMS	Interim Joint Tactical Information Distribution System Message Specification
JCM	JTIDS COMSEC Module
JCMO	Joint Communications Security Management Office
JFILL	JTIDS Fill
JICO	Joint Interface Control Officer
JNL	Joint Tactical Information Distribution System Network Library
JPI	JTIDS Product Improvement
JSMP	JTIDS Signal Message Processor
JSS	Joint Interface Control Officer (JICO) Support System (JSS)
JSTARS	Joint Surveillance Target Attack Radar System
JTAGS	Joint Tactical Ground Station
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JU	JTIDS Units
KCP	Keyer Control Panel
KDSUAS	Key Distribution Support User Application Software
KEK	Key Encryption Key
KEYMAT	Keying Material
KMGA	Key Management Goal Architecture
KMI	Key Management Infrastructure
KOA	KMI Operating Account
KOAM	KMI Operational Account Manager
KP	Key Processor
KPK	Key Production Key
LAK	Link 16 Alaska
LCC	Amphibious Command Ship
LCM	LVT Crypto Module (MIDS)
LCMS	Local Communications Security Management Software
LCU	Load Control Unit
LHD	Landing Helicopter Dock an amphibious assault ships

LMD	Local Management Device
LVT	Low-Volume Terminal
MCE	Modular Control Equipment
MGC	Management Client (KMI)
MHz	Megahertz
MIDS	Multifunctional Information Distribution System
MIL-STD	Military Standard
MKEK	Master KEK
MPMSS	Mission Planning Management Support System
MROC	Minimum Required Operational Capability
msec	Millisecond
MSEC	Message Security
NAG	NAG is not an acronym but an NSA scheme
NATO	North Atlantic Treaty Organization
NCMS	Naval Communications Security Material System
NCS	National Command System
NDF	Network Design Facility
NEW	Network Enabled Weapons
NHPS	Navy High Powered Ship Terminal
NIMROD	NIMROD MRA4 Aircraft
nm	Nautical Mile
NOFORN	Not Releasable to Foreign Nationals
NORAD	North American Aerospace Defense Command
NPG	Network Participation Group
NSA	National Security Agency
NSACF	National Security Agency Central Facilities
NTR	Network Time Reference
OEM	Original Equipment Manufacturer
OPTASK LINK	Operational Tasking Data Link
OTNK	Over-the-Network Keying
PC	Personal Computer
PPLI	Precise Participant Location and Identification
PRSN	Primary Services Node (KMI)
PSIAM	Programmable scalable Information Assurance Module
PSN	Product Source Node (KMI)
PVM	Partitioned Variable Mode
RAM	Random Access Memory
RAIDER	A robust tactical communications system
RASKL	Really Simple Key Loader
ROB	Reserve On Board

ROBE	Roll-On Beyond Line of Sight Equipment
RTT	Round-Trip Timing
SCO	Santa Cruz Operations Operating System
SDS	Secure Data Transfer Device 2000 System
SDU	Secure Data Unit
SHAR	Royal-Navy-Sea-Harrier
SHORAD	Short Range Air Defense
SKL	Simple Key Loader
SMP	Signal Message Processor
SSA	Software Support Activity
STE	Secure Telephone Equipment
STT	Small Tactical Terminal
TAMPS	Tactical Aircraft Mission Planning System
TAOC	Tactical Air Operations Center
TAOM	Tactical Air Operations Module
TCP/IP	Transmission Control Protocol/Internet Protocol
TCU	Transmission Security/Communications Security Unit
TDL	Tactical Data Link
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Key
THAAD	Terminal High Altitude Area Defense
TKL	Tactical Key Loader
TrKEK	Transmission Key Encryption Key
TSEC	Transmission Security key identifier for Link 16
TSK	Transmission Security Key
UAS	User Application Software
US	United States
USA	US Army
USAF	US Air Force
USCENTCOM	US Central Command
USEUCOM	US European Command
USMC	US Marine Corps
USN	US Navy
USNORTHCOM	US Northern Command
USPACOM	US Pacific Command
USSOUTHCOM	US Southern Command
UTC	Coordinated Universal Time
W	Watt
WII	Waveform Instance Identifier

PART II-DEFINITIONS

Allied. A term used within this document to refer to operations between or keys used by the United States and member nations of a treaty organization (i.e., NATO), coalition, or combined force.

Black Key. An encrypted key.

Common Signal Processor (CSP). A product of the Joint Tactical Information Distribution System Class II Terminal Embedded Crypto Card Product Improvement Program.

Common Tier 3 (CT3) software. Data transfer device software used to fill all operational crypto devices.

Common Variable Mode (CVM). The mode of operation in which the same key is used for traffic encryption/decryption and transmission security.

Controlled Cryptographic Item (CCI). Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements.

Controlling Authority (CONAUTH). The official responsible for directing the operation of a cryptonet and managing the operational use and control of keying material assigned to the cryptonet. In Link 16, the official responsible for the proper security and use of a COMSEC short title.

Coordinated Universal Time (UTC). A measure of time that conforms, within a close approximation, to the mean diurnal rotation of the Earth and serves as the basis of civil timekeeping. Used to establish the valid cryptographic interval for Link 16 keying material.

Cryptographic Network (cryptonet). A collection of operational units whose data is being protected from all others by the encryption process provided from a single crypto key. Link 16 can operate with multiple cryptonets simultaneously. Note that multiple network participation groups can be operating in the same cryptonets.

Cryptographic Variable Logic Label (CVLL). The tie between short titles and network design. Also, the tie between secure data unit memory locations and network design.

Current Cryptographic Period Designator (CCPD). A one-bit parameter used to determine what set of keys is in use on a particular day. See Table A-4.

Data Management Device (DMD). A USAF software package that runs on a PC or Palm top that creates the management information for the Common Tier 3. It also will interface with the KOV-21 to act as a fill device. The DMD will operate with or without the KOV-21.

Data Transfer Device (DTD). The common name for AN/CYZ-10.

Data Transfer Device Encrypted Key. Key data that results from a key being encrypted with a transmission key encryption key.

DS-101. The Electronic Key Management System standard for electronic key transfer.

DS-101 Key Encryption Key. The key encryption key used in the KGV-8 and CDH to encrypt/decrypt keys transferred via DS-101.

Electronic Key Management System Key Encryption Key. The key encryption key used to encrypt data for transport from one COMSEC account to another.

End Cryptographic Unit (ECU). The generic name for any crypto device. Sometimes referred to as Tier 4 in EKMS.

End Cryptographic Unit Key Encryption Key (ECU KEK). Key data that results from a key being encrypted with an ECU KEK.

Fighter Data Link (FDL). Multifunctional Information Distribution System (MIDS) Low-Volume Terminal 3. The MIDS variant used in F-15s.

Front-End System (FES). A receive-only Link 16 terminal. The CDH is embedded on the transmission security/communications security unit. The unit can be set from the front panel to be either DS-101 or DS-102.

Interim Joint Tactical Information Distribution System Message Specification (IJMS). The message standard for Class I Joint Tactical Information Distribution System terminals. IJMS is still used in NATO and some USAF E-3 aircraft.

Interoperability Standards for Electronic Key Management Systems. Replaces the previous standards: DS-100, DS-101, DS-102, and NSA 87-27.

Joint Interface Control Officer (JICO). Combatant Commander's responsible officer to plan, manage and execute all data link operations within the CCMD area of responsibility. CCMD JICOs provide the network design criteria and distribute OPTASK LINK planning guidance to Service Components and Service Network Design Facilities.

Joint Tactical Information Distribution System Network Library (JNL). Compendium of Joint Tactical Information Distribution System networks, normally distributed as a single magnetic media item.

Joint Tactical Information Distribution System Unit Data. An operations task link data field.

Key. In this context, "key" refers to the information bits that specify the generation of protection hiding bit stream, which is used to hide the intelligent information transmitted through the communication system. In many older documents, the name crypto variable is used. The Director, NSA, has directed that key be used instead of crypto variable.

Key Distribution Support User Application Software (KDSUAS). USN user application software to work with the local communications security management software in the Electronic Key Management System to provide support data and keys to the Common Tier 3 on a data transfer device from the local management device/key processor.

Key Encryption Key (KEK). The key used to encrypt or decrypt other keys for transmission or storage.

Key Processor (KP). The Key Processor is a trusted component of the EKMS. It performs cryptographic functions, including encryption and decryption functions for the account, as well as key generation, and electronic signature operations. A KOK-22A."

Keyer Control Panel (KCP). A device used to set the memory address into which the key goes. The load control unit is a KCP in a box for USN aircraft ship use on flight deck. The KCP is required for DS-102 key fill. The DS 101 key fill does not require a KCP; the software in the AN/CYZ-10 sets the memory location.

Link 16. A jam-resistant, line-of-sight tactical data and voice communication system with relative navigation capabilities.

Load Control Unit (LCU). The LCU mechanically encapsulates a keyer control panel.

Local Communications Security Management Software (LCMS). This software runs on the local management device to control and utilize the key processor. A basic part of Tier 2.

Local Management Device (LMD). The central element of Tier 2 accounts in the EKMS system. (A dedicated PC loaded with LCMS.)

Megahertz (MHz). One million cycles per second.

Message Security (MSEC). A Cryptovariable that is used by a Link 16 unit to encrypt message data for transmission on Link 16
Military Standard (MIL-STD) 6016A. The document defining message formats and data elements for Link 16 messages.

Multifunctional Information Distribution System Low-Volume Terminal (MIDS-LVT). The Link 16 transceivers designed for integration in various airborne and air defense platforms. Current variants are from 1 – 12. The major variants are MIDS LVT(1), MIDS LVT(2), and MIDS LVT(3). All others are minor modifications of one of these three.

National Distribution Authority. The NSA key production and distribution authority.

National Security Agency Central Facilities (NSACF). Key Production Tier 0.

Network Participation Group (NPG). A unique list of applicable Link 16 messages used to support an agreed technical function without regard to subscriber identities. This list is a means of transmitting a common set of Link 16 messages to all interested users. Frequently used NPGs include electronic warfare, C2, network synchronization, etc.

Network Time. Network time is that time maintained by a JU designated as the Network Time Reference (NTR) and is the common time reference with which all other JTIDS Units (Jus) synchronize.

NSA Specification 90-2A. The THORNTON smart fill data standard. It is a DS 101 base standard with the special fields required for the THORNTON smart fill defined.

Operational Tasking Data Link (OPTASK LINK). The US message text format that provides detailed instructions regarding tactical data link operations, including information required to establish these links.

Partitioned Variable Mode (PVM). The mode of operation in which a different message security traffic encryption key is used to secure specific compartmented data that is used for other Link 16 data and for Link 16 transmission security for traffic encryption/decryption and transmission security.

Random Access Memory (RAM). Computer memory provides the main internal storage available to the user for programs and data. This is sometimes referred to as “volatile” memory. There are eight memory locations in the secure data unit that are volatile and used for traffic encryption keys and over-the-air rekey

key encryption keys. The USA Multifunctional Information Distribution System variant (MIDS-LVT(2)) has 64 RAM locations.

RED Key. An unencrypted key.

Reserve On Board (ROB). The amount of key required to be present at an account for future use because that account will not be able to communicate with the account that generates the key for a period of time.

Round-Trip Timing (RTT). Messages sent and received that are used to accurately assess the distance between terminals.

Secure Data Transfer Device 2000 System (SDS) KIK-20. The SDS was developed by NSA. It is designed to securely receive, store, and transfer electronic data between compatible communication equipment.

Secure Data Unit (SDU). The functional name for the THORNTON cryptographic equipment used in Link 16 terminals. Link 16 SDUs include the KGV-8/A/B/C in the Joint Tactical Information Distribution System Class II, the E-GLD in some of the USA systems, and the CDH in the common signal processor card and in the signal message processor card of the Multifunctional Information Distribution System.

Signal Message Processor (SMP). The processing card of the Multifunctional Information Distribution System terminal that processes signals and raw messages.

Simple Key Loader (SKL) AN/PYQ-10. A handheld data transfer device used to transfer keys between Electronic Key Management System devices.

Software Support Activity (SSA). Each COMSEC software package is required by the Director, NSA, to have an SSA established to correct problems and add new capabilities.

Tactical Aircraft Mission Planning System (TAMPS). The system used to build the network to be installed in the Link 16 system. The National Command System (NCS) for the US Army and the command and control processor (C2P) for the ships perform similar functions. TAMPS is offline, whereas C2P and NCS are online and exercise communication functions as well.

THORNTON. The project name that refers to the KGV-8 equipment and the THORNTON embedded products.

Tier 0. The Central Facility at NSA. This facility is capable of doing Tier 1 functions. It also forms the bridge between the United States and other countries.

Tier 1. The Service key production, distribution, and accounting facility. This tier has large production capabilities for the electronic key but none for the physical key. Personnel from each Service staff Tier 1.

Tier 2. Designation of the local account holder. The local communications security management software running on the local management device connected to the key processor makes up the backbone of this tier.

Tier 3. This is the user level of the system. The user holds and uses the AN/CYZ-10, AN/PYQ-10(C), RaSKL, or SDS-2000 to fill Tier 4 equipment.

Tier 4. This tier is generally identified with the end cryptographic units.

Time Slot. The minimum burst of communication possible in Link 16. One or more Link 16 messages are transmitted in each time slot. A time slot is 7.8125 msec in duration and 128 time slots are transmitted each second, or 1,536 time slots within each 12-second frame.

Traffic Encryption Key (TEK). The key used to encrypt plain text or to super encrypt previously encrypted text and/or to decrypt cipher text. Within the Link 16 system, TEK provides both transmission security and message security.

Transmission Key Encryption Key (TrKEK). The key encryption key used to decrypt keys in the AN/CYZ-10, AN/PYQ-10(C), RaSKL, or SDS-2000 data transfer device.

Transmission Security (TSEC). A cryptovariable that is used by a Link 16 unit to determine the duration of jitter within the time slot, message data scrambling, the frequency on which to transmit, as well as the pseudorandom noise with which the received transmission was masked by the transmitter. Transmission Security/Communications Security Unit (TCU). Part of the front-end system that is a controlled cryptographic item and handles the interface to the CDH.

Transmission Security Key (TSK). Keying material that provides transmission security in a system. In the Link 16 system, the TEK performs both the TEK and TSK functions. Although the Electronic Key Management System provides the selection of the TSK, there is no way to distinguish the TSK from the TEK within the Link 16 terminals. The Director, NSA, generally considers the TSK to be a lower risk than the TEK. The Link 16 terminal will very likely use any key it is given to perform, as with the TEK function. Therefore, all traffic keys should be designated as TEKs and never as TSKs.

(INTENTIONALLY BLANK)