CRYPTOME

24 December 2009

KGV-72 Key Management Plan (KMP) – Plan 3
D42563
19 May, 2008
UNCLASSIFIED // FOR OFFICIAL USE ONLY

(U) Blue Force Tracking Type 1 COMSEC Upgrade Program
KGV-72 Key Management Plan 3

(U) OPR assigned KMP number: 2006-30

(U) National Security Agency (NSA) Program Manager (PM) Contact Information:

Ken Olthoff
NSA, Information Assurance Directorate
I824, Combat Applications Division
(410) 854-6462
k.olthof@radium.ncsc.mil

National Security Agency
Attn: Ken Olthoff
9800 Savage Road, Suite 6733
Ft. Meade, MD 20755-6733

Source:

https://abop.monmouth.army.mil/busopor27-2009.nsf/Solicitation+By+Number/D3312D5DF943167785257540008OB4C1/$File/Att+006+KGV72+KMP3+19May08.pdf

(U) Blue Force Tracking Type 1 COMSEC Upgrade Program
KGV-72 Key Management Plan 3

(U) OPR assigned KMP number: 2006-30

(U) National Security Agency (NSA) Program Manager (PM) Contact Information:

Ken Olthoff
NSA, Information Assurance Directorate
I824, Combat Applications Division
(410) 854-6462
k.olthof@radium.ncsc.mil

National Security Agency
Attn: Ken Olthoff
9800 Savage Road, Suite 6733
Ft. Meade, MD 20755-6733

(U) Government PM & contact information:

Dominic Satili
Deputy PdM for Blue Force Tracking
US Army PEO C3T, PM FBCB2
(732) 427-2817
Dominic.Satili@us.army.mil

US Army
Program Manager Force XXI Battle Command Brigade and Below
Attn: Dominic Satili, SFAE-C3T-FB-BFT
Ft. Monmouth, NJ 07703-5601

(U) REVISION/CHANGE RECORD

FOR DOCUMENT NO. D42563

Date	Document Section	Change Description
27 Mar 2007	All	Initial submission of KMP3
14 September 2007	All	Incorporated comments from Consolidated comments
5 November 2007	All	Incorporated comments from Consolidated comments
25 January 2008	All	Incorporated comments from Consolidated comments
1 February 2008	All	Incorporated comments from Consolidated comments
12 March 2008	All	Incorporated comments from Consolidated comments
19 May 2008	All	Incorporated comments from Consolidated comments

Table of Contents

(U) Tables of Tables

(U) Table of Figures

1 (U) INTRODUCTION

(U//FOUO) This document is the Key Management Plan 3 (KMP 3) for the Force XXI Battle Command Brigade and Below (FBCB2) Blue Force Tracking (BFT) System as part of the Type 1 Communications Security (COMSEC) Upgrade Program.

1.1 (U) Scope

(U//FOUO) This document details the key management processes for key ordering, generation, distribution, storage, accounting, compromise, recovery and destruction. It is intended to support the National Security Agency (NSA) evaluation for product endorsement and certification.

1.2 (U) Acronyms

(U//FOUO) The definitions of acronyms used in this KMP are provided in Appendix A.

1.3 (U) References

(U//FOUO) Applicable reference documents are contained in (U) Table 1.3-1.

(U) Table 1.3-1 Reference Documents

Document ID	Document Name Government Publications	Document Date
	A Guide to Acquiring Keys and Signatures	23 August 2004
NSTISSI 4006	Controlling Authorities for COMSEC Material	02 Dec 91
IAD Management Directive 10	Cryptographic Key Protection	7 July 2005
DI-MISC-90019B	(Data Item Description) Key Management Plan Guidance	29 May 2002
V34-01-2001	DRAFT Telecommunications Security Requirements Document (TSRD) for the FBCB2 Blue Force Tracking System L-Band Secure Message Processing Program Crypto Upgrade	31 May 2006
EKMS 217 0N48116	EKMS Benign Techniques Specification, Revision G - 21	December 2001
W15P7T-04-D- G205	FBCB2 Statement of Work (SOW) for Phase III	11 Jan 2006
D42508	FBCB2 BFT Type 1 KGV-72 KMP 1	13 May 2006
D42534	FBCB2 BFT Type 1 KGV-72 KMP 2	6 Sep 2006
D38985	Force XXI Battle Command Brigade and Below (FBCB2) Blue Force Tracking (BFT) Type 1 Communication Security (COMSEC) Upgrade System Subsystem Specification (SSS)	27 Jan 2006
CNSS Instruction No. 4009	National Information Assurance Glossary	June 2006
CNSS Instruction No. 3021	Operational Security Doctrine For The AN/CYZ-10/10A, Data	Sep 2002

Document ID	Document Name Government Publications	Document Date
	Transfer Device (DTD)	
NSTISSI 4003	Reporting and Evaluating COMSEC Incidents	02 Dec 91
NSTISSI 4004	Routine Destruction and Emergency Protection of COMSEC Material	02 Dec 91
NSTISSI 4005	Safeguarding Communications Security (COMSEC) Facilities & Materials	Aug 97
TB 380-41	Technical Bulletin Security : Procedures for Safeguarding, Accounting and Supply Control of COMSEC material	15 March 2006
D39903	Type 1 COMSEC Upgrade – Interface Control Document (ICD)	27 Jan 2006
BFT UIC	Unified INFOSEC Criteria (UIC) for Blue Force Tracking Device (SECRET)	30 March 2006
ARMY-UPA-032-04	User Partnership Agreement	2 Nov 2004
0N682380	Sierra II Software Design Document, Para, 4.4.4	2004
	Key Specification for the Application Specific JOSEKI Split Seed (SECRET//NOFORN)	26 Feb 03
	KGV-72 Interface Control Document	TBD
	L-Band Blue Force Tracking Type III Cryptographic Implementation	TBD
	Interface Control Document (ICD) for Army Simple Key Loader (SKL) KGV-72 Interface	TBD

	Non-Government Publications	
	BFT Key Management Proposal	March 2006
	Force XXI Battle Command Brigade and Below (FBCB2) Blue Force Tracking (BFT) Type 1 Communication Security (COMSEC) Key Management CONOPS Version 1.0	3 Feb 2006

1.4 (U) BACKGROUND

(U//FOUO) Currently, the FBCB2 BFT system can process only unclassified messages. The communications conduit for BFT is a Comtech commercial L-Band satellite service provider, which uses only commercial Type 3 bulk encryption. The capability to transmit classified messages over a commercial link requires encryption methods that are NSA approved as Type 1.

(U//FOUO) The United States Army Program Manager (PM) for FBCB2 initiated development of a cryptographic application to meet a requirement in the FBCB2 Operational Requirements Document and Mission Needs Statement for Beyond Line of Site/Near Line of Site Family of Systems, which states that FBCB2 is to be able to process Secret information. This requirement

is currently met in the terrestrial version of FBCB2 using Single Channel Ground and Airborne Radio System (SINCGARS) and Enhanced Position Location Reporting System (EPLRS) radios. The current mobile satellite version of FBCB2 BFT does not meet the requirement to transmit Secret information.

(U//FOUO) This cryptographic application was initiated on 15 March 2006 under delivery order 0010 of Contract W15P7T-04-D-G205. A User Partnership Agreement (ARMY-UPA-032-04) was signed by PM FBCB2 on 2 November 2004 and by NSA on 25 October 2004. PM FBCB2, subordinate to the Program Executive Office, Command, Control and Communications-Tactical (PEO C3T) at Fort Monmouth, New Jersey, is the Army Project Manager Office (PMO). The Communications Electronics Command (CECOM) at Fort Monmouth is the contracting agency.

(U//FOUO) The purpose of this cryptographic application is to allow BFT to create, process, transmit and receive classified messages up to the Secret level. In order to accommodate this purpose, the cryptographic application is an inline End Cryptographic Unit (ECU), known to the BFT Secured Message Processing System as a KGV-72, at each end of the commercial satellite link.

2 (U) CRYPTOGRAPHIC APPLICATION DESCRIPTION

2.1 (U) Cryptographic Application Descriptions

(U//FOUO) The new BFT KGV-72 cryptographic application will provide an inner Type 1 link encryption capability/layer. The Type 1 capability/layer will be in addition to the existing Type 3 capability/layer which is currently being provided by the satelitte provider's transceiver hardware and software. The outer layer Type 3 commercial cryptography provides obfuscation of the message, since Comtech Mobile Datacom, the commercial satellite communications provider, routinely secures other transmitted information via Type 3 encryption.

(U//FOUO) A single KGV-72 design will be used at two BFT message transmission points, i.e., the BFT Network Operations Center (NOC) and the tactical mobile vehicles. In the mobile ground or airborne platform, KGV-72 will function as a Platform Encryption Device (PED). At the NOC, the KGV-72 software will function as a NOC Encryption Hardware (NEH). The PED and NEH share the same hardware and software.

(U//FOUO) The KGV-72 incorporates the Sierra™ II cryptographic engine developed by Harris Corporation. The Sierra™ II Application-Specific Integrated Circuit (ASIC) meets all of the requirements for the NSA Cryptographic Modernization Program and completed NSA Type 1 certification in September 2004. Figure 2.1-1 provided a physical illustration of the KGV-72.

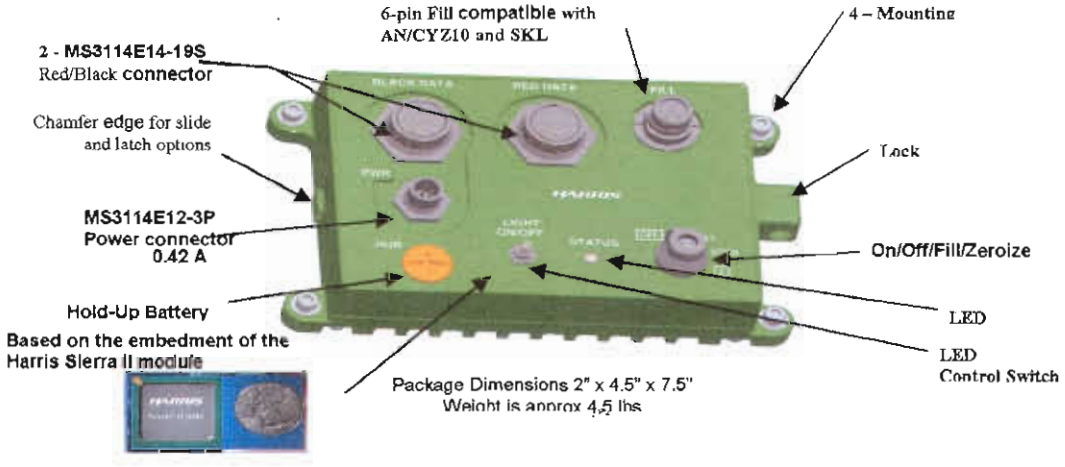

Figure 2.1-1 Physical Illustration of the KGV-72

2.2 (U) Confidentiality

(U//FOUO) The KGV-72 is designed to meet Type 1 protection standards. It is designed to provide high confidentiality protection to communication traffic. It is also designed to protect storage of internal keys at a classification level up to and including Secret.

(U//FOUO) COMSEC methods assure confidentiality for the KGV-72 software and for the messages processed by and transmitted through the KGV-72. KGV-72 supports encryption and decryption of data via NSA approved algorithms. Currently the specific algorithms that are implemented for BFT KGV-72 include MEDLEY for data encryption, JOSEKI for software encryption, and ACCORDION for key encryption.

(U//FOUO) The embedded Sierra II ASIC uses JOSEKI decryption/encryption to protect the confidentiality of classified KGV-72 software. The KGV-72 is loaded with JOSEKI encrypted software and classified algorithms at the Harris factory prior to shipment. The Type-1 initialization process for the KGV-72 is defined in the Sierra II Software Design Document submitted by Harris to NSA for certification in 2004.

2.3 (U) Integrity

(U//FOUO) The KGV-72 employs multiple mechanisms designed to prevent or detect intrusion. These mechanisms, along with the use of Electronic Key Management System (EKMS) devices for the transmittal of key, assure a high degree of confidentiality and integrity of information as it is being transmitted between the NOC and vehicle. In addition, a cryptographic data integrity function is applied to all message traffic. Details regarding the KGV-72 data integrity are classified and are discussed in the Theory of Compliance (TOC) and whitepaper entitled Traffic Encryption/Decryption Algorithm/Mode Study for the BFT KGV-72, dated 04 December 2006.

(U//FOUO) Integrity of all downloaded software files, policy files and configuration files is implemented as a part of the Type 1 signature process.

2.4 (U) Non-Repudiation

(U//FOUO) The KGV-72 does not provide non-repudiation.

2.5 (U) Access Control

(U//FOUO) The KGV-72 is an Unclassified Controlled Cryptographic Item (CCI) when unkeyed. As such, access to KGV-72 must be controlled. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4001 and individual Service procedures define the specific requirements that must be met). When keyed the KGV-72 takes on the highest classification of the keys loaded.

(U//FOUO) The KGV-72 supports access control via role- and device-based authentication. Any consequent allowance or restriction of functionality is based on the success of that authentication. There is a single method of authorized KGV-72 authentication known as Communicator Authentication that will authenticate a bound red side host computer to be able to communicate user data to the KGV-72's red side data interface. The authenticator is based upon the external split of the internally generated Key Local Unique Key (KLUK), defined in section 8.1 of this KMP. The details of the Communicator Authentication process are considered out of scope of this KMP and can be reviewed in the KGV-72 Theory of Equipment Design and Operation.

(U//FOUO) The KGV-72 key access will be accomplished/controlled in compliance with applicable NSA certified specifications and Service specific guidelines. The following NSA specifications, documents or policies are pertinent to this section:

- NSTISSI 4003: Reporting and Evaluating COMSEC Incidents, 02 Dec 91
- NSTISSI 4004: Routine Destruction & Emergency Protection of COMSEC Material, 02 Dec 91
- NSTISSI 4005: Safeguarding Communications Security (COMSEC) Facilities and Materials, Aug 1997
- NSA Memo I221-068-2004, Key Handling, 09 Dec 04

2.6 (U) Availability

(U//FOUO) The KGV-72 does not provide a robust anti-jam capability. The L-Band network uses redundant satellite services to overcome loss of the primary signal.

2.7 (U) Planned Upgrades

(U//FOUO) Any future upgrades to the system will be covered in a revision to the BFT KMP.

2.8 (U) Level of Protection

(U//FOUO) The KGV-72 is designed to meet Type 1 protection standards. It is designed to provide high confidentiality protection to communication traffic. It is also designed to protect storage of internal keys, JOSEKI key, operational keys (Traffic Encryption Key (TEK) and Key Encryption Key (KEK)), and application software at a classification level up to and including Secret.

2.9 (U) Development, Maintenance, Test, Operation, And Contingency Key Management

(U//FOUO) The current key management structure provides key management support for the KGV-72. The BFT program follows existing key management structure policies and procedures for development, maintenance, test, operation and contingency key management support. Refer to Section 4.0 for key types, functions and specifications.

3 (U) COMMUNICATIONS ENVIRONMENT

(U//FOUO) This section describes the communications environment for BFT KGV-72.

3.1 (U) Network Environment

(U//FOUO) The BFT network is a hub and spoke architecture, consisting of mobile vehicles, NOC, and a commercial satellite system. Vehicles send unicast messages via satellite to the NOC (see Figure 3.1-1). The NOC processes the messages and broadcasts multicast messages via satellite to multiple vehicles. Figure 3.1-2 illustrates the BFT physical architecture with the KGV-72.

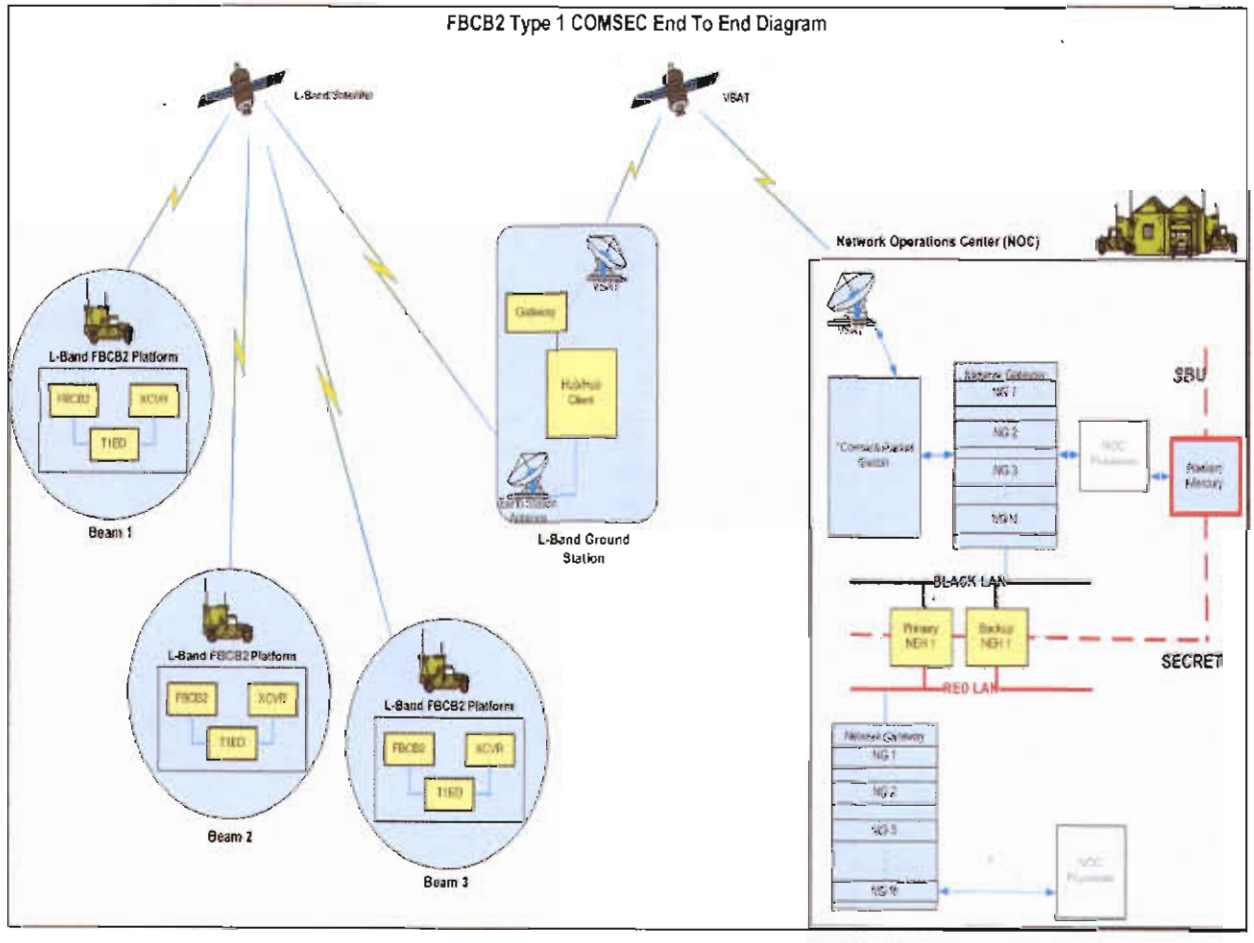

Figure 3.1-1 BFT Architecture with KGV-72 in the Mobile Units

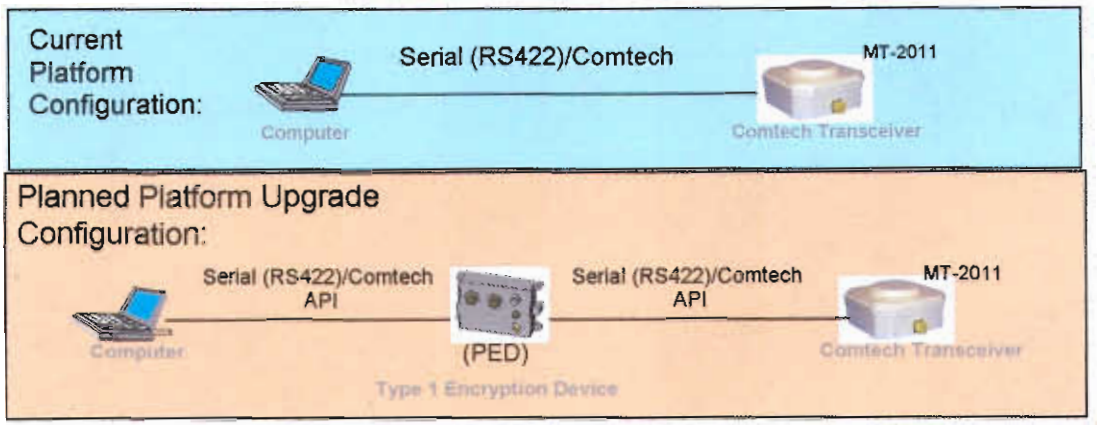

Figure 3.1-2 BFT with KGV-72 Physical Configuration

(U//FOUO) Comtech Mobile Datacom Corporation is the current satellite network provider for BFT. The Comtech network provides communication transmission security using Type 3 algorithm.

(U//FOUO) The BFT system includes five NOCs, which process, meter, and route message traffic to/from vehicles located in specific geographic areas of responsibility. One NOC will act as the primary default hub for vehicles co-located in a region, while another NOC will act as the backup when the primary NOC is unavailable. Vehicles communicate with the NOC via satellite beams. Vehicles may be in an area covered by more than one satellite beam; however, vehicles lock onto only one beam at a time. Typically the satellite beam providing the strongest signal is used to communicate with the NOC. Each satellite beam has a capacity to support hundreds of vehicles. The beam capacity is a function of the number of vehicles and the frequency of position reporting. This frequency varies with BFT software versions. Figure 3.1-3 illustrates the current and planned NOC configuration.

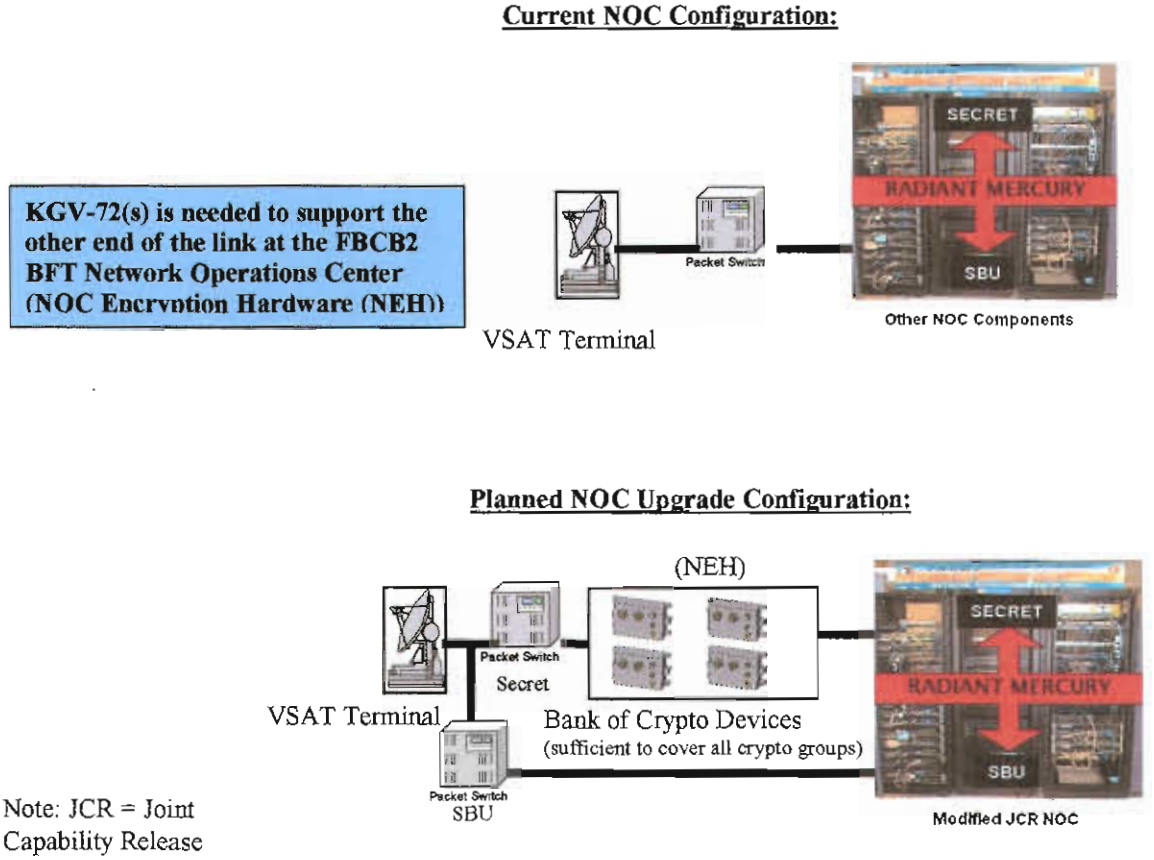

Figure 3.1-3 BFT Architecture with KGV-72 in the NEH

3.2 (U) Methods

3.2.1 (U) Wired Communications

(U//FOUO) At the BFT vehicle platforms, the KGV-72 interfaces between the BFT computer and the Comtech transceiver using an RS-422 serial connection. At the NOC, the KGV-72 interfaces with NOC switches and/or routers using an Ethernet connection. The NOC is

contained in a physically secured building, while the KGV-72 on the mobile platform is installed in either a combat vehicle or aircraft.

3.2.2 (U) Wireless Communications

(U//FOUO) The KGV-72 is used to secure end-user message data that is transmitted over a commercial L-Band satellite network. Data required for infrastructure support of the secure messaging, e.g., keys and KGV-72 software upgrades, are not transmitted over the satellite network.

3.3 (U) Allies

(U//FOUO) The KGV-72 is currently releasable to US forces, including the Joint U.S. Command. There are no current plans to release the KGV-72 to Allied or Coalition forces, although it is a possibility that future release of the KGV-72 will include the Combined Communication Electronic Board (CCEB) community. Key availability and distribution to CCEB community would be coordinated at that time.

4 (U) KEY MANAGEMENT PRODUCTS AND SERVICE REQUIREMENTS

4.1 (U) Key Types/Uses and Their Specifications

(U//FOUO) The BFT KGV-72's key management products and services requirement information for key types/uses and functions and their specifications are provided in(U) Table 4.1-1.

(U) Table 4.1-1 FBCB2 BFT KGV-72 Key Types/Uses and Specifications

	Test Keys		Operational Keys		
Key Type	**TEK**	**KEK**	**TEK**	**KEK**	**JOSEKI**
Key Purpose	Bench/ Maintenance Over-the-Air-Test	Bench/ Maintenance Over-the-Air-Test	BFT traffic encryption	Protection of BFT TEK	Protection of Algorithms
Key Short Title	To Be Assigned By Tier 1 To Be Assigned By Tier 1	To Be Assigned By NSA To Be Assigned By Tier 1	To Be Assigned By Tier 1	To Be Assigned at generation at Tier 2	To Be Assigned Upon Final Software Release*
Key Algorithm	MEDLEY	ACCORDION	MEDLEY	ACCORDION	JOSEKI
Key Format	Electronic	Electronic	Electronic	Electronic	Electronic
Key Generation Responsibility	Tier 1	Tier 1	Tier 1	Tier 2 LMD/KP	Central Facility
Key Quantities	10	10	20 short titles	1 per COMSEC account	1 per software Release
ECU Quantities	400	400	60K	60K	60K
Cryptoperiod	TBD	TBD	TBD**	TBD**	TBD
Classification	Unclassified	Unclassified	SECRET	SECRET	SECRET
Date Needed	15 May 07	15 May 07	1 Aug 08	1 Aug 08	1 Aug 07*
Controlling Authority	PM FBCB2	PM FBCB2	BFT Global NOC	Commander over the Tier 2 Account	NSA

*(U//FOUO) JOSEKI has been generated by NSA and provided to Harris Corporation. Short Title is to be associated at Harris Corporation upon final software release. Harris Corporation will provide notification to NSA for ECU assignment and distribution purposes.

(U//FOUO) Key support required for lifetime of ECU.

(U//FOUO) ** Crypto periods for operational TEK & KEK are listed in the classified version of this KMP3.

(U//FOUO) Information deleted.

(U//FOUO) The process for supersession requires a few steps:

- All platforms on the crypto-net are filled with the next TEK prior to expiration of the current TEK (while continuing to use the current TEK).
- At the beginning of the next crypto period, the NOC will be programmed to start using the new TEK for all outgoing messages for that crypto-net.
- All vehicle platforms in the crypto-net will receive the message encrypted with the new TEK.
    - If the vehicle was filled with the next appropriate TEK, that platform would be able to decrypt the message and inform the host computer that a new traffic key was used on the crypto-net. The host computer will then be capable of determining that a new key fill had occurred on the crypto-net and command the KGV-72 to begin using the new TEK for all outgoing messages on that crypto-net. The host computer will also command the KGV-72 to purge the replaced TEK.
    - If the vehicle was not filled with the appropriate next TEK, that platform would not be able to decrypt the message and drop all subsequent incoming messages encrypted with the new TEK. The platform will continue to use the existing TEK for all outgoing messages.

(U//FOUO) If the NOC were to immediately purge any replaced TEKs from the NEH KGV-72, the NEH KGV-72 would not be able to decrypt any messages from any vehicles that were overlooked during the fill process. Thus, the NOC operator would not be able to detect that a vehicle would require the new TEK. To circumvent that, the NOC will retain (but not use for any outgoing messages) the TEK for an additional unit of time in order to decrypt any messages from any straggling platform. The message would contain the identity of the unit representing that platform, and indicate the geographical location. The message will prompt the NOC operator to dispatch an appropriate Signal Support Specialist to verify the unit's identity and provide the appropriate TEK.

4.2 (U) Existing Key Specification Information

(U//FOUO) The FBCB2 BFT KGV-72 will utilize the existing Pre-Placed Key Format for High Assurance Internet Protocol Encryption Interoperability Standard (HAIPE-IS) Key Specification, dated 27 Jul 05, for traffic key generation. A production instruction set in the Key Generation (KG) Rules that are associated with this key specification do exist already and is currently tied to the HAIPEA equipment type and available today at the Tier 1 and the Tier 2 level Local Management Device (LMD)/Key Processor (KP).

(U//FOUO) The FBCB2 BFT KGV-72 will utilize the existing bit structure for an ACCORDIAN KEK that is currently associated with the equipment type IFFKEK.

(U//FOUO) There will have to be a modification to the KG Rules to add an equipment type KGV72. The TEK for this equipment type will point to the production instruction that is currently associated with the HAIPEA equipment type. The KEK for this equipment type will point to the production instruction that is currently associated with the IFFKEK equipment type.

5 (U) KEY MANAGEMENT PRODUCTS AND SERVICES ORDERING

(U//FOUO) Key Management Ordering and Receipt Responsibilities at the NOC include:

- Key ordering, receipt and loading is handled via the EKMS,
- Encryption and Decryption of Messages, including key order requests,
- Issuing and receiving Re-key Commands and Verifying Responses, and
- Maintenance of the Key Management Database.

(U//FOUO) The KGV-72 key management will support the migration of the current Key Mangement System. The current Key Management System that will support the FBCB2 BFT Secure Message Processing System for L-Band will have a minimum capability of: Local COMSEC Management Software (LCMS) v 5.0 with Common User Application Software (CUAS) v 5.03 and Automated Communications Engineering System (ACES) version 1.9. Migration to the Key Management Infrastructure is met by meeting the minimum requirements of the EKMS baseline (LCMS 5.1 and CUAS 5.1).

5.1 (U) JOSEKI

(U//FOUO) JOSEKI is used to decrypt the classified cryptographic applications. The private element used to initialize the ECU has been generated by NSA/Y1, Central Facility and distributed to Harris Corporation for ECU assignment.

The current short tile that has been assigned to the initial version of KGV-72 software is [USKAE B9927 ED1]. Harris Corporation will notify NSA/Y1 as well as the BFT Army program office of any new short title associations prior to the release of any future versions of KGV-72 software.

Tier 0 will be responsible for the distribution of the JOSEKI private element to an authorized Tier 2 COMSEC accounts by way of the Tier 1 common message server. A DS-100-1 key tag is required on the JOSEKI private element prior to distribution to the KGV-72. It is assumed that EKMS will mandate that a key tag is placed on the private element prior to the Bulk Encrypted Transaction (BET) between Tier 1 and Tier 2. The JOSEKI private element will then be distributed from Tier 2 to the KGV-72. This approach requires the use of a AN/CYZ-10(V)3 Data Transfer Device (DTD) or AN/PYQ-10(C) Simple Key Loader (SKL) (or another approved Tier 3 Fill Device – according to Section 7 paragraph 4) to load ECUs with the private element.

(U//FOUO) The complete creation and distribution process consists of three stages: A) Creating and signing* the software image; B) Creating the private element; and C) Distributing the private element to the end user Tier 2 account. For new equipment fielding, the primary mode to load the private element is at the Original Equipment Manufacturer's (OEM) location. The primary mode of distribution of the Operational JOSEKI private element to support sustainment activities (example – Type 1 reinitializing) will be through the EKMS to the Tier 2 LMD/KP. In addition, some manual accounts, without an LMD/KP may require distribution of the JOSEKI Split via approved Key Transfer methods (shipment or approved communications transmission).

*Signing the software images requires the OEM to submit code to NSA. NSA will return the signed software image back to the OEM. The KGV-72 will contain NSA's public certificate.

(U//FOUO) After a KGV-72 is fielded, distribution of JOSEKI splits is performed via EKMS to the Tier 2 LMD/KP. Proper handling of the private element is controlled in accordance with the FBCB2 Operational Security Doctrine and the KGV-72 Theory of Compliance Appendix A – Fielding and Maintenance Support Concept of Type 1 Initialization.

(U//FOUO) After the KGV-72 is filled with the JOSEKI private element, the ECU will continue to be handled as a CCI. The KGV-72 will be handled at the same security level as the highest level TEK or KEK that is filled. If the KGV-72 is un-keyed, then the ECU remains Unclassified but handled at CCI even if it contains the private element.

5.2 (U) Key Encryption Keys

(U//FOUO) KGV-72 KEKs will be generated at the Tier 2 LMD/KP level. The KEK is utilized by CUAS in the LMD/KP to encrypt the TEK and for the ECU to decrypt the black TEKs. Red KEKs will be delivered via the approved Tier 3 Key Transfer Device (according to Section 7 paragraph 4) to the KGV-72. A KEK will be shared within a single BFT Global Network Operational Center (BGN) or within a brigade unit. The KEK will only be utilized to protect the TEKs while in transit from Tier 2 LMD/KP to the KGV-72.

(U//FOUO) The KGV-72 can support both ACCORDION 1.3 and ACCORDION 3.0 algorithms. However, by direction of the NSA, the KGV-72 will currently support a KEK based upon the ACCORDION 1.3 algorithm.

5.3 (U) Traffic Encryption Keys

(U//FOUO) A shared traffic key (using the MEDLEY algorithm) will be used for each traffic crypto-net that is part of the BFT L-Band Secure Message Processing System. There are two enclaves: a tactical enclave and a testing enclave. There are three BGNs to support tactical operations, and two NOCs to support testing and training operations.

Tactical Enclave	Testing/Training Enclave
BGN1 – Ft. Monmouth	NOC1 – CTSF in Ft. Hood
BGN2 – Ft. Carson	NOC2 – NGMS in DH
BGN3 – Ft. Hood	

(U//FOUO) The following (U) Table 5.3-1 shows the number of anticipated tactical crypto-nets required per theater by Area of Responsibility supporting current operations. These Areas of Responsibility (AOR) are supported by BGN1, BGN2, and BGN3.

(U) Table 5.3-1 Operational Crypto-Nets

Theater	No. of CNs	Areas of Responsibility
CENTCOM	2	OEF, OIF
PACOM	1	AK-HI
EUCOM	3	Africa, EUR, Kosovo
NORTHCOM	1	CONUS
SOUTHCOM	1 or more	1 or more missions
ASIA	1	Korea

(U//FOUO) A particular BGN will have prime responsibility over a particular subset of AORs. However, all BGNs will have the responsibility to serve as a backup to another BGN in the event that the primary BGN for a particular set of AORs failed. Therefore, BGN1, BGN2, and BGN3 all need to share crypto-net data (key variables, crypto period dates, member vehicle data, etc.). This includes that during the key ordering process, all three BGNs must be on the distribution for each short title required to support operations. For more information regarding the BFT hub and spoke architecture, refer to section 3.1 of this KMP.

(U//FOUO) In addition, there are currently two test crypto-nets as part of NORTHCOM that are supported by NOC1 and NOC2. The purpose of this enclave is to support any training exercises involving the NOC1 at the Central Technical Support Facility (CTSF) in Ft. Hood, TX. This enclave also supports any testing during the development and improvement cycles of the KGV-72 and host platform. NOC2, located at the Northrop Grumman Mission Systems Dominguez Hills (NGMS DH) facility in Carson, CA, will support any internal FBCB2 testing. This enclave will not use any operational keys. Only test and training keys will be used.

(U//FOUO) Since NOC2 will not have an LMD/KP, NOC2 will require either Tier 1 or Tier 2 to generate all test keys. The test keys will be transferred from point of generation to NOC2 via approved Key Transfer methods (shipment or approved communications transmission).

(U//FOUO) Operational TEKs will be generated at Primary Tier 1 Segment (PT1S) Ft. Huachuca AZ. Under current plans, a single TEK per crypto-net will be shared for each area of responsibility. Future plans may include breaking up an area of responsibility into multiple crypto-nets according to mission and/or split picture capability.

5.4 (U) Key Ordering

(U//FOUO) All key orders are coordinated by the Tier 2 COMSEC Account through CSLA Ft. Huachuca, AZ, the Army's Service Authority. The Commander for each local generating Tier 2 LMD/KP account will be the Controlling Authority (CONAUTH) for the KEKs. The BFT Global NOC is the CONAUTH for TEKs. The CONAUTH works with CSLA for key distribution through EKMS. Figure 5.4-1 represents this process for ordering TEKs.

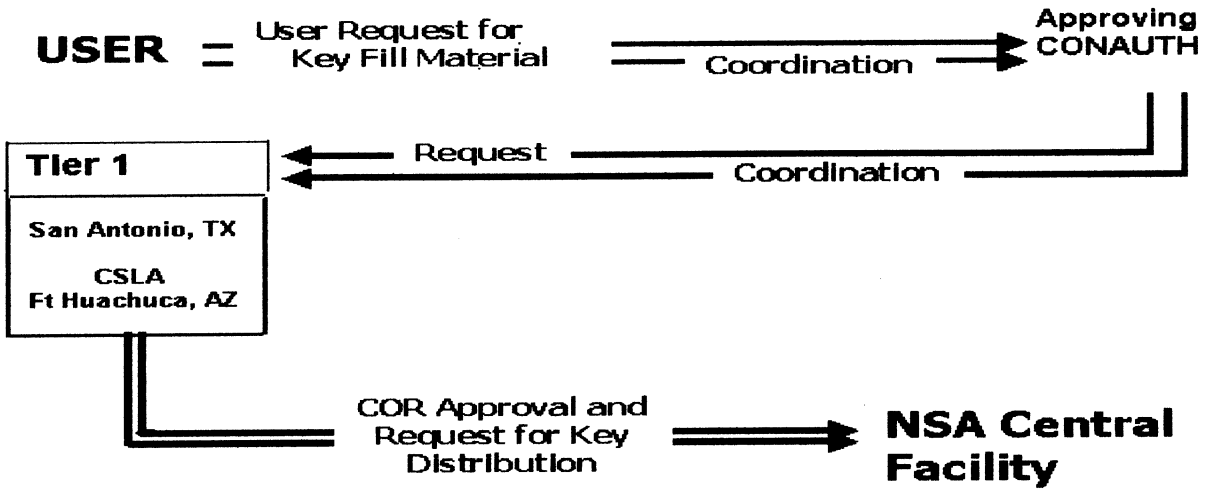

Figure 5.4-1 Key Order Process for Operational Keys

6 (U) KEY MATERIAL GENERATION

(U//FOUO) Responsibility to generate operational keys is dictated by key type and key CONAUTH as defined in Table 4.1-1. Test keys will be generated at Tier 1 or Tier 2 and distributed to NOC 1 & 2 via approved Key Transfer methods (shipment or approved communications transmission).

7 (U) KEY DISTRIBUTION

(U//FOUO) All BFT key variables will be distributed electronically via EKMS. Key generation and distribution will be initiated by the CONAUTH. KEKs will be generated and distributed from the local Tier 2 LMD/KP. Tier 1 will generate TEKs and distribute them to authorized Tier 2 LMD/KPs via a BET.

(U//FOUO) The Tier 2 LMD/KP will encrypt the BFT TEK in the locally generated KGV-72 KEK. The black TEK will be exported to an ACES workstation via floppy or Compact Disk. The ACES workstation will perform the necessary crypto-net planning functions and apply an appropriate DS-100-1 key tag to the black TEK. The black TEK with the DS-100-1 key tag will then be loaded into the approved Tier 3 Key Transfer Device.

(U//FOUO) Distribution of the red KEK will be accomplished from the Tier 2 LMD/KP into the approved Tier 3 Key Transfer Device. The Tier 3 operator will then fill the red KEK directly into the KGV-72 via DS101 fill port.

(U//FOUO) Protection of the red KEK and JOSEKI private elements will be in accordance with service specific directives. Additional requirements for the protection and distribution of JOSEKI splits are listed in the following paragraph.

(U//FOUO) To support sustainment activities, distribution of the JOSEKI private element is performed via EKMS. ECUs will be returned by the field level maintainer to a secured maintenance location for Type 1 re-initialization. The JOSEKI private element can be hand receipted to the approved Special Electronics Device Repairer. The approved Tier 3 Fill Device (in accordance with Section 7 paragraph 4) containing the JOSEKI split shall be controlled in accordance with the FBCB2 Operational Security Doctrine.

(U//FOUO) The use of TrKEK (Transfer Key Encryption Key) wrapping will be applied to protect the red KEK. The use of a TrKEK is incompatible with the KGV-72 KEK encryption of a TEK; therefore the KEK encrypted TEK shall never be wrapped by the TrKEK.

(U//FOUO) Policy dictates that if the red KEK is stored on the same DTD or SKL fill device as the TEKs that are encrypted in the respective KEK, then that respective black TEK must be considered red. Information Assurance Directive (IAD) Management Directive 10 requires the protection of key during distribution. Since the TrKEK wrapped KEK will be loaded on the same approved fill device as the respective TEK only during the periods required when distributing the KEK, a waiver will be requested by PM FBCB2 to the NSA against IAD Management Directive 10.

(U//FOUO) The KGV-72 will be tested with the use of the DTD and the SKL. The legacy Common Fill Devices (such as the KOI-18, KYK-13, and KYX-15) are not compatible with the KGV-72 and cannot be used as fill devices for KGV-72 key material. Other Tier 3 recognized fill devices (such as the KIK-20 Secure DTD2000System (SDS)) are approved for use, however will not be officially tested by the Army PMO. In addition, the Tier 3 operator will have the

capability to use a profile as part of the SKL User Application Software (UAS) version 5.0 to load key material for the KGV-72 equipment.

(U//FOUO) As part of the remove and replace procedures of the KGV-72, the field level maintainer (Signal Support Specialist - example, in the Army the MOS is 25U) will evacuate the KGV-72 to the Electronic Maintenance Shop (ELM). The ELM is a secured controlled trailer that includes approved handling and storage of CCI. The operator will sign over the KGV-72 to the field level maintainer as part of the chain of custody. At the ELM, the field level maintainer will sign over the KGV-72 to the Special Electronics Devices Repairer (example, in the Army the MOS is 94F).

(U//FOUO) The Special Electronics Devices Repairer will confirm fault and check for tamper. The Sierra Terminal Program will be provided to the ELM to allow checks for fault and tamper. If the tamper was not triggered, and there is no other fault, other than JOSEKI private element being cleared due to operator failure, then the Special Electronics Devices Repairer will Type 1 re-initialize the KGV-72. The device then must be returned to the unit following the reverse chain of custody per unit established procedures.

(U//FOUO) During combat operations, the ELM is located in the Brigade Support Area (BSA). The BSA is a secured area away from austere environments and has COMSEC capabilities. The Special Electronics Devices Repairer will be authorized to hand receipt for the JOSEKI private element from the EKMS Manager.

(U//FOUO) Any question for the FBCB2 system that cannot be answered by the FBCB2 Operator Technical Manual (TM 11-7010-326-10) should be fielded to the FBCB2 Help Desk. The FBCB2 Help Desk can inform the ELM EKMS Manager what short title was established for the JOSEKI private element for that KGV-72. The NSA Central Facility shall make KGV-72 JOSEKI private elements available through the EKMS from Tier 0 to Tier 1. The JOSEKI private element will then be delivered to the units ELM Tier 2 account by way of the Tier 1 message server.

(U//FOUO) If the Special Electronics Devices Repairer confirms that the fault is beyond operator clearing the private element, or in the event that the tamper was triggered, or some other compromise, then the KGV-72 will be evacuated to the Tobyhanna Forward Repair Activity (FRA).

(U//FOUO) The FRA will have cleared technicians that will be approved and trained to detect and perform tamper recovery activities. Standard logistics for maintenance will be followed for the faulted KGV-72 to establish if the chain of continuous custody was broken. If the KGV-72 was found to be maliciously tampered, the device will follow established investigative channels. Otherwise, the FRA technician will have the capability to reload KGV-72 software, recover tamper resets, and Type 1 reinitializes the KGV-72.

(U) If the default is beyond the FRA capabilities and scope, the device can be returned back to Tobyhanna Army Depot.

8 (U) KEY MANAGEMENT PRODUCTS AND SERVICES STORAGE

8.1 (U) Internal Key Storage

(U//FOUO) Internal to the KGV-72, Mission/Operational keys (KEKs & TEKs) are filled and stored with their DS-100-1 Key Tags. Mission keys are stored internally encrypted in a KLUK. The KLUK is internally generated within the Sierra II and is used to encrypt the KEKs and TEKs. The KLUK is stored in key RAM within the Sierra II. The KLUK is unique per KGV-72 and cannot be distributed outside the Sierra II. The KGV-72 can store at a minimum 100 TEKs and 100 KEKs in the Sierra II. Red keys exist only within the Sierra II module and only while the cryptographic sub-system requires their functionality. The KGV-72 can hold up to 50 mission keys as active in the unencrypted state.

8.2 (U) Key Storage Compliance

(U//FOUO) BFT KGV-72 keys will be stored in compliance with applicable NSA certified specifications and Service specific guidelines. The following NSA specifications, documents and policies are pertinent to this section:

- NSTISSI 4003: Reporting and Evaluating COMSEC Incidents, 02 Dec 91
- NSTISSI 4004: Routine Destruction and Emergency Protection of COMSEC Material, 02 Dec 91
- NSTISSI 4005: Safeguarding Communications Security (COMSEC) Facilities & Materials, Aug 97
- Key Specification for the Application Specific JOSEKI Split Seed, 26 Feb 03, (SECRET//NOFORN)

8.3 (U) Key Access Control

(U//FOUO) BFT KGV-72 key access will be accomplished in compliance with applicable NSA certified specifications and Service specific guidelines. The following NSA specifications, documents and/or policies are pertinent to this section:

- NSTISSI 4003: Reporting and Evaluating COMSEC Incidents, 02 Dec 91
- NSTISSI 4004: Routine Destruction and Emergency Protection of COMSEC Material, 02 Dec 91
- NSTISSI 4005: Safeguarding Communications Security (COMSEC) Facilities & Materials, Aug 97
- Key Specification for the Application Specific JOSEKI Split Seed, 26 Feb 03, (SECRET//NOFORN)

9 (U) KEY MANAGEMENT ACCOUNTING

(U//FOUO) BFT KGV-72 key accountability and key destruction will be accomplished in compliance with applicable NSA certified specifications and the Service specific guidance for safeguarding, accounting, destruction and Supply Control of COMSEC Material. The following NSA specifications, documents and/or policies are pertinent to this section:

- NSTISSI 4003: Reporting and Evaluating COMSEC Incidents, 02 Dec 91
- NSTISSI 4004: Routine Destruction and Emergency Protection of COMSEC Material, 02 Dec 91
- NSTISSI 4005: Safeguarding COMSEC Facilities & Materials, Aug 97
- Key Specification for the Application Specific JOSEKI Split Seed, 26 Feb 03, (SECRET//NOFORN)

10 U) BENIGN FILL

(U//FOUO) The KGV-72 will not support benign fill. Request for Approval for Cryptographic Key Protection Policy for: KGV-72 (FBCB2 Blue Force Tracking L-Band Crypto) – Action Memorandum" was evaluated and approved by NSA on 6 March 2007. BFT will implement Black Key Wrap Techniques for TEKs. Integrity of red KEK fill process will be in compliance with current service specific policy and delivered to the KGV-72 via a separate distribution path from the black TEKs when mission/security allows.

11 (U) KEY COMPROMISE MANAGEMENT AND RECOVERY

11.1 (U) Compromise Evaluation and Determination

(U//FOUO) The compromise/loss of a key would necessitate the issuance of a COMSEC incident report. The COMSEC incident report is sent as an action to the appropriate CONAUTH, to the Director, National Security Agency, ATTN: I413, Fort George Meade, MD, and to the appropriate Service, Department or Agency authorities in accordance with NSTISSI 4003 or applicable service directives.

(U//FOUO) The CONAUTH reviews the incident report and consults with all affected command elements within the coverage area regarding the necessity to perform compromise recovery operations. Once the CONAUTH has made an evaluation, the ultimate decision to perform the recovery operation is made by the CONAUTH.

11.2 (U) Compromise Recovery

(U//FOUO) Recovery from the compromise of a key, as stated in NSA doctrine, calls for notification of all affected command elements to update their compromised key list. The appropriate Support Center can update the Routing Table to route messages from compromised KGV-72 IDs to the Battalion (BN), Brigade (BDE), Theater of Operations, or NOC for determination of actions required due to the receipt of a message from a compromised KGV-72.

(U//FOUO) Since the global system utilizes various TEKs according to area of responsibility, the loss of an individual KGV-72 will not necessarily affect the security of other KGV-72s outside the current Mission group or crypto-net. If it is determined that the risk of compromise of the TEK is above the acceptable risk criterion, then a TEK rollover for that unique TEK is required to recover. This TEK rollover exercise would necessitate the re-keying of each KGV-72 within the crypto-net served by any compromised TEK. Each KGV-72 would be manually re-keyed using the authorized key fill device(s) to perform re-keying with the next available TEK. Every edition of the TEK will contain three segments of key. A single segment of the edition will be designated and loaded as the primary segment for that edition's crypto period. The additional two segments would remain in the DTD or SKL (or any approved Tier 3 Key Transfer Device) and be utilized in the event of emergency supersession (compromise recovery). Necessary coordination and agreement on the selection and use of the next TEK would occur between the current Mission group or crypto-net COMSEC custodian(s) and the appropriate EKMS Manager at the NOC. The capability to readily perform TEK rollover in the field is dependent upon the availability of the key fill device(s) and the key fill operator to perform rollover. If there is no available TEK in the fill device, then the key fill device would be returned to the appropriate Tier 2 LMD/KP, which would be used to load the next TEK into the key fill device. The fill device would be physically returned to the field of operations where the key fill operator would use it to load the replacement TEK into each KGV-72 in the crypto-net.

(U//FOUO) In the case of a KEK compromise, then both the KEK and the TEK that the KEK protected must be rolled-over to the next KEK and TEK, as appropriate. In addition to the TEK

rollover described in the preceding paragraph, either KEK rollover using a replacement KEK in the key fill device would be necessary, or the key fill device would need to be returned to the appropriate BDE LMD/KP to load the key fill device with the next KEK. After the loading of the replacement KEK into the key fill device, then the fill device would be returned to the field of OPS where it would be used to fill the KGV-72.

11.3 (U) KGV-72 Physical Compromise and Recovery

(U//FOUO) The KGV-72 incorporates several features to mitigate the impact of its physical compromise:

1) The KGV-72 front panel Zeroization capability so that if activated, then it will erase the Primary and any Secondary TEKs and KEKs.
2) Additionally, the KGV-72 stores its KEK in its protective microprocessor (Security Module).
3) The KGV-72 also incorporates a physical tamper detection mechanism to protect against compromise. When physically tampered, the ECU will zeroize all resident key material to include the JOSEKI algorithm, thus requiring Type-1 initialization (reload of JOSEKI, as described in Section 5.1).

(U//FOUO) To further mitigate the risk of physical compromise, the FBCB2 BFT system will implement the Over-The-Air-Rekey techniques of the commercial satellite system as described in the L-Band Blue Force Tracking Type III Cryptographic Implementation White Paper. This NSA approved technique will re-key the L-Band transceiver of the outer commercial encryption, not the KGV-72.

11.4 (U) Key Recovery Compliance

(U//FOUO) Key recovery will be in accordance with applicable NSA certified specifications and Service specific guidelines. The NSA specification, NSTISSI 4006: Controlling Authorities for COMSEC Material, 02 Dec 91, is pertinent to this section.

11.5 (U) Re-keying Post Zeroization

(U//FOUO) The design/implementation technique with which the KGV-72 meets the need to become an unclassified CCI device is to zeroize the box. This may be necessary in an operational environment when soldiers need to leave the vehicle unattended in an unsecured environment. Zeroization is done either by moving the front panel knob to the "Z" position (this action requires a 2-step pull-to-turn to prevent accidental zeroization), or sending software "zeroize all" command. Note: the software command also requires a second step by the user to confirm action in the host computer to prevent accidental zeroization.

(U//FOUO) To restore the KGV-72 to operational condition after zeroization, the authorized key-fill operator would use an authorized key fill device (DTD or SKL) to reload the TEK and KEK.

12 (U) APPENDIX–A - DEFINITION OF ACRONYMS

Acronym	Definition
ACES	Automated Communications Engineering Software
AOR	Area of Responsibility
ASIC	Application Specific Integrated Chip
BDE	Brigade
BET	Bulk Encrypted Transaction
BFT	Blue Force Tracking
BGN	BFT Global NOC
BN	Battalion
BSA	Brigade Support Element
CCEB	Combined Communications-Electronic Board
CCI	Controlled Cryptographic Item
CECOM	Communication Electronic Command
CENTCOM	Central Command
CF	Central Facility
COMSEC	Communications Security
CONAUTH	Controlling Authority
COR	Central Office of Record
CSLA	Communications Security Logistics Activity
CTSF	Central Technical Support Facility (CTSF)
CUAS	Common User Application Software
DTD	Data Transfer Device
ECU	End Cryptographic Unit
EKMS	Electronic Key Management System
ELM	Electronic Maintenance Shop
EPLRS	Enhanced Position Location Reporting System
EUCOM	Europe Command
FBCB2	Force XXI Battle Command Brigade and Below
FRA	Forward Repair Activity
HAIPE-IS	High Assurance Internet Protocol Interoperability Standard
ICD	Interface Control Document or Development
KEK	Key Encryption Key
KLUK	Key Local Unique Key
KMP	Key Management Plan
KG	Key Generation
KGV-72	Programmable In-Line Encryption Device
LCMS	Local COMSEC Management Software
LMD/KP	Local Management Device/Key Processor
NEH	NOC Encryption Hardware
NOC	Network Operations Center

NORTHCOM	Northern Command
NGMS DH	Northrop Grumman Mission Systems Dominguez Hills
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
PACOM	Pacific Command
PED	Platform Encryption Device
PEO	Program Executive Office
PEO C3T	Program Executive Office Command, Control, and Communications – Tactical
PM FBCB2	Program Manager for FBCB2
PM	Program Manager
PMO	Program Management Office
PT1S	Primary Tier 1 Segment
RSHC	Red-Side Host Computer
SAID	Security Association Identifier
SDS	KIK-20 Secure DTD2000System
SINCGARS	Single Channel Ground and Airborne Radio System
SKL	Simple Key Loader
SOUTHCOM	Southern Command
SOW	Statement of Work
SSS	System Subsystem Specification
TEK	Traffic Encryption Key
TOC	Theory of Compliance
TrKEK	Transfer Key Encryption Key
TSRD	Telecommunications Security Requirements Document
UAS	User Application Software
UIC	Unified INFOSEC Criteria