

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**CNSS Instruction No. 3032
August 2003**



**(U) OPERATIONAL SECURITY DOCTRINE
FOR
THE VIASAT INTERNET PROTOCOL (VIP) CRYPTO
VERSION 1 (KIV-21)**

This document contains information exempt from mandatory disclosure under the FOIA. Exemption 3 applies.

The information contained herein that is marked U//FOUO is for the exclusive use of the DoD, other U.S. government, and U.S. contractor personnel with a need-to-know. Such information is specifically prohibited from posting on unrestricted bulletin boards or other unlimited access applications, and to an e-mail alias.

This document prescribes minimum standards. Your department or agency may require further implementation.

Approved for Release by NSA on 09-25-2024, FOIA Case # 51573

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Committee on National Security Systems

CNSSS Instruction No. 3032



National Manager

1. (U) The Committee on National Security Systems Instruction No. 3032, "Operational Security Doctrine for VIASAT Internet Protocol (VIP) Crypto Version 1 (KIV-21)," prescribes the minimum security standards for the protection and use of the KIV-21.
2. (U) CNSSS Instruction No. 3032 is effective upon receipt. It replaces the Interim Systems Security Doctrine for this equipment, which should be destroyed.
3. (U) Representatives of the Committee on National Security Systems may obtain additional copies of this Instruction at the address listed below.
4. (U) U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.
5. (U//~~FOUO~~) Questions regarding this Instruction may be sent directly to the National Security Agency,

Michael V. Hayden
 MICHAEL V. HAYDEN
 Lieutenant General, USAF

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

CNSS Secretariat National Security Agency . 9800 Savage Road STE 6716 : Ft Meade MD 20755-6716

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

CNSS Instruction No. 3032

**(U) OPERATIONAL SECURITY DOCTRINE
FOR
VIASAT INTERNET
PROTOCOL (VIP) CRYPTO VERSION 1 (KIV-21)**

TITLE	SECTION
INTRODUCTION	I
SYSTEM & EQUIPMENT DESCRIPTION.....	II
CLASSIFICATION AND ACCOUNTING LEGEND CODE.....	III
PERSONNEL RESPONSIBILITIES.....	IV
KEYING.....	V
REMOTE MANAGEMENT.....	VI
SECURITY REQUIREMENTS	VII
INSTALLATION & MAINTENANCE	VIII
INSECURITY REPORTING	IX

SECTION I - (U) INTRODUCTION

1. **(U) Purpose** - This doctrine contains minimum security standards for the protection and use of the VIP Crypto Version 1 (KIV-21) equipment, associated components, and COMSEC material.

NOTE: (U) Implementing Services, Departments, and Agencies of the U.S. Government may direct more stringent standards than those stated in this instruction, but may not delete, reduce, or diminish any standard contained herein.

2. **(U) Application** - The provisions of this doctrine apply to all Services, Departments, and Agencies of the U.S. Government and their contractors who handle, distribute, account for, store, or use the KIV-21 and its associated COMSEC material.

3. **(U) Doctrinal Conflicts** - Any conflicts between the requirements of this instruction and any other national-level doctrine shall be identified and submitted for resolution to DIRNSA, ATTN:

[Redacted]

4. **(U) Waivers** - Requests for exceptions to any of the requirements of this instruction must be approved, on a case-by-case basis, prior to implementation. Each such request must present a complete operational justification and must be submitted through appropriate Service, Department, or Agency channels to DIRNSA, ATTN: [Redacted]

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

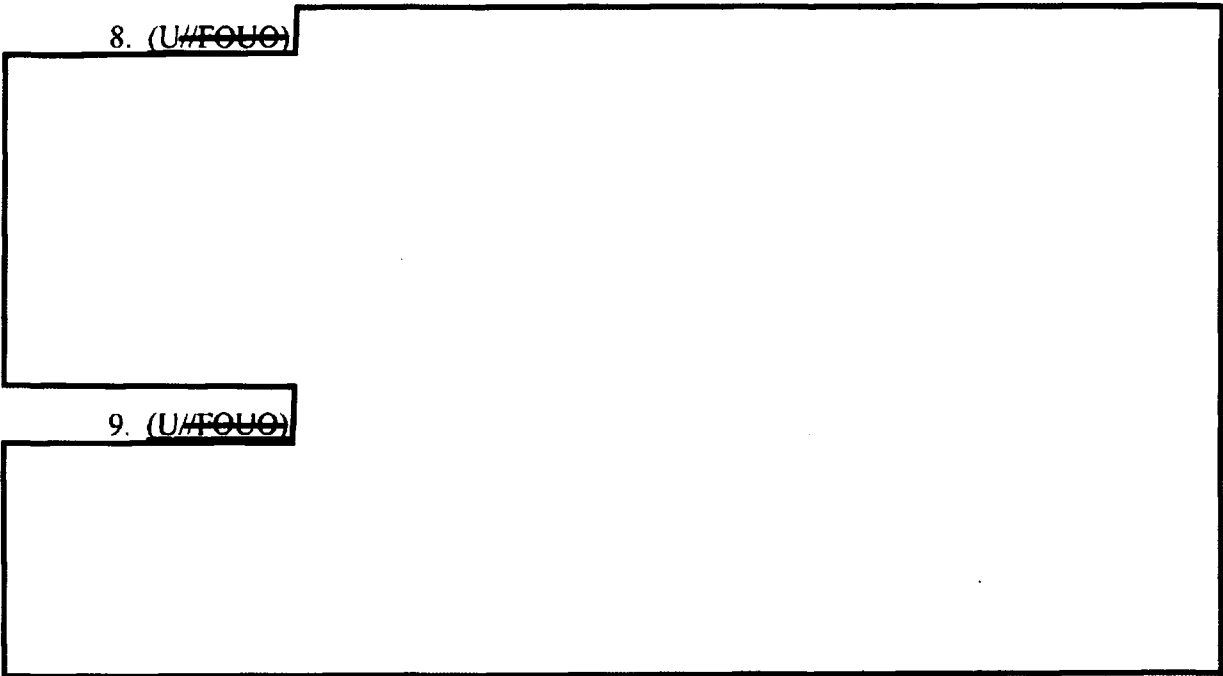
CNSS Instruction No. 3032

- 5. (U) References - References are listed in ANNEX A.
- 6. (U) Acronyms - Acronyms are expanded in ANNEX B.
- 7. (U) Definitions - NSTISSI No. 4009 Revision 1 definitions apply to this doctrine. Additional specialized terms applicable to this doctrine are defined below:
 - a. (U) Designated Approving Authority (DAA) - An executive with authority and ability to evaluate the mission business case and budgetary needs for a national security information system.
 - b. (U) Local Authority (LA) - The individual responsible for network configuration of all KIV-21s within his/her domain.
 - c. (U) Security Administrator (SA) - The individual responsible for maintaining, monitoring, and controlling functions performed by the KIV-21.

SECTION II - (U) SYSTEM & EQUIPMENT DESCRIPTION

8. (U//FOUO)

9. (U//FOUO)



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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

CNSS Instruction No. 3032

a. (U) **Physical Size and Weight** - The KIV-21 is 15.3 x 3.4 x 17 inches, and weighs 12 pounds.

b. (U//~~FOUO~~)
[Redacted]

c. (U//~~FOUO~~)
[Redacted]

SECTION III - (U) CLASSIFICATION

10. (U//~~FOUO~~)
[Redacted]

a. (U)
[Redacted]

b. (U)
[Redacted]

11. (U//~~FOUO~~)
[Redacted]

SECTION IV - (U) PERSONNEL RESPONSIBILITIES

12. (U) **Personnel** - Individuals requiring access to the KIV-21 equipment must possess an appropriate U.S. Government security clearance and must have a need-to-know for the equipment.

a. (U) **Designated Approving Authority** - As addressed in NSTISSI No. 1000, the DAA determines the acceptable level of residual risk for national security information systems that are secured by the KIV-21.

b. (U) **Local Authorities** - LAs are responsible for net planning and the network and security configuration of all KIV-21s in their domains.

c. (U) **Security Administrator** - SAs are responsible for maintaining, monitoring, and controlling all functions performed by each KIV-21. SAs interface with both the COMSEC Custodians and LAs for management of keying material. SAs are authorized to load key into KIV-21s. SAs configure the security functions of the KIV-21 by:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

CNSS Instruction No. 3032

- (U) Receiving for all KIV-21 key from the COMSEC Custodian.
- (U) Keying and zeroizing the KIV-21.
- (U) Ensuring that approved procedures are followed for storing, protecting, and handling KIV-21 key.
- (U) Notifying the COMSEC Custodian of reportable COMSEC incidents and ensuring that recovery actions are taken, when appropriate.
- (U) Retrieving and reviewing KIV-21 security audit data.
- (U) Specifying if and how often the KIV-21 audit log must be reviewed.

NOTE: (U//~~FOUO~~)



- (U) Prescribing the physical security requirements for KIV-21 terminal areas.

13. (U) COMSEC Custodian - The COMSEC Custodian is responsible for ordering, receiving, and safeguarding KIV-21 key until it is issued to the SA.

14. (U) Combining Functions - Where it is operationally necessary, the functions of LA and SA may be combined and vested in one individual. Where necessary, the COMSEC Custodian may perform one or both these roles.

SECTION V - (U) KEYING

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

15. (U) Types of Key - The KIV-21 uses two types of COMSEC key:

a. (U//~~FOUO~~)



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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

CNSS Instruction No. 3032

NOTE: (U//~~FOUO~~)

[Redacted]

b. (U//~~FOUO~~)

[Redacted]

16. (U//~~FOUO~~)

[Redacted]

NOTE: (U) NSTISSI No. 4006 states the responsibilities of commanders and civil department and agency officials who serve as CAs for COMSEC key and provides guidance for fulfilling those responsibilities.

17. (U//~~FOUO~~)

[Redacted]

NOTE: (U//~~FOUO~~)

[Redacted]

18. (U) Cryptoperiods

a. (U//~~FOUO~~)

[Redacted]

NOTE: (U//~~FOUO~~)

[Redacted]

b. (U//~~FOUO~~)

[Redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

CNSS Instruction No. 3032

c. (U//~~FOUO~~) [Redacted]

SECTION VI - (U) REMOTE MANAGEMENT

19. (U) Hyper Text Transfer Protocol (HTTP) - The KIV-21 can be http-managed from either the Plaintext (PT) side or the Ciphertext (CT) side, but PT-side management is not encrypted. CT-side management is encrypted between the KIV-21 fronting the Manager and the managed KIV-21. If an Encryptor Manager (EM) Workstation is used for network management, operation must be controlled as follows:

- a. (U//~~FOUO~~) [Redacted]
- b. (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]
- (U//~~FOUO~~) [Redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

CNSS Instruction No. 3032

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

SECTION VII - SECURITY REQUIREMENTS

20. (U) Accountability

a. (U//~~FOUO~~)

[Redacted]

NOTE: (U) NAG No. 71 sets forth the minimum security standards for safeguarding, controlling, and using the EKMS Local Management Device/Key Processor, and NSTISSI No. 3021 sets forth the minimum security standards for the protection and use of the DTD.

b. (U//~~FOUO~~)

[Redacted]

NOTE: (U) Operational KIV-21 TEKs and over-the-air test key are marked "CRYPTO", but bench test key and classroom training key are not. Keying material used for classroom training only is UNCLASSIFIED, is accounted for locally, and may be used indefinitely.

c. (U//~~FOUO~~)

[Redacted]

21. (U) Transportation - KIV-21s must be zeroized prior to shipment between COMSEC accounts and must be shipped in accordance with provisions of NSTISSI No. 4001. If pre-shipment zeroization is not possible, keyed equipment must be transported by means authorized by NSTISSI No. 4005 for the highest classified key they contain.

22. (U//~~FOUO~~)

[Redacted]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

CNSS Instruction No. 3032

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

SECTION VIII - (U) INSTALLATION & MAINTENANCE

23. (U) General Standard - KIV-21s must be maintained in accordance with provisions of NSTISSI No. 4000, which prescribes minimum standards for COMSEC equipment maintenance and maintenance training, and delineates responsibilities and establishes procedures for enforcing those standards.

24. (U//~~FOUO~~)

[Redacted]

a. (U//~~FOUO~~)

[Redacted]

b. (U//~~FOUO~~)

[Redacted]

c. (U//~~FOUO~~)

[Redacted]

d. (U//~~FOUO~~)

e. (U//~~FOUO~~)

[Redacted]

f. (U//~~FOUO~~)

g. (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

[Redacted]

NOTE: (U//~~FOUO~~)

[Redacted]

25. (U) Zeroization - Malfunctioning KIV-21s must be returned unkeyed to the manufacturer (i.e., the KIV-21 must be actively zeroized). Zeroization and verification procedures follow:

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

CNSS Instruction No. 3032

- a. (U//~~FOUO~~)
- b. (U//~~FOUO~~)
- c. (U//~~FOUO~~)
- d. (U//~~FOUO~~)

26. (U) Warranty Support - Malfunctioning KIV-21s must be zeroized and returned to ViaSat, Inc., for repair or replacement. Any attempt at local repair invalidates the manufacturer's warranty.

SECTION IX - INSECURITY REPORTING

- 27. (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)
- (U//~~FOUO~~)

2 Encls: a/s

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

ANNEX A

(U) REFERENCES

(U) The following national-level references are cited in this Doctrine:

- a. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, January 1999.
- b. NSTISSI No. 4002, Classification Guide for COMSEC Information, 5 June 1986
- c. NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000.
- d. NSTISSI No. 4001, Controlled Cryptographic Items, July 1996.
- e. NSTISSI No. 4006, Controlling Authorities for COMSEC Material, 2 December 1991.
- f. NAG No. 71, Interim Operational System Security Doctrine for the Local Management Device/Key Processor (LMD/KP) (KOK-22), April 1997.
- g. NSTISSI No. 3021, Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device (DTD), September 1997.
- h. NSTISSI No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 1997.
- i. NSTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, 11 March 1987.
- j. NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training, January 1998.
- k. NSTISSI No. 7000, Tempest Countermeasures for Facilities, 29 November 1993.
- l. NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, 2 December 1991.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

ANNEX B

(U) ACRONYMS

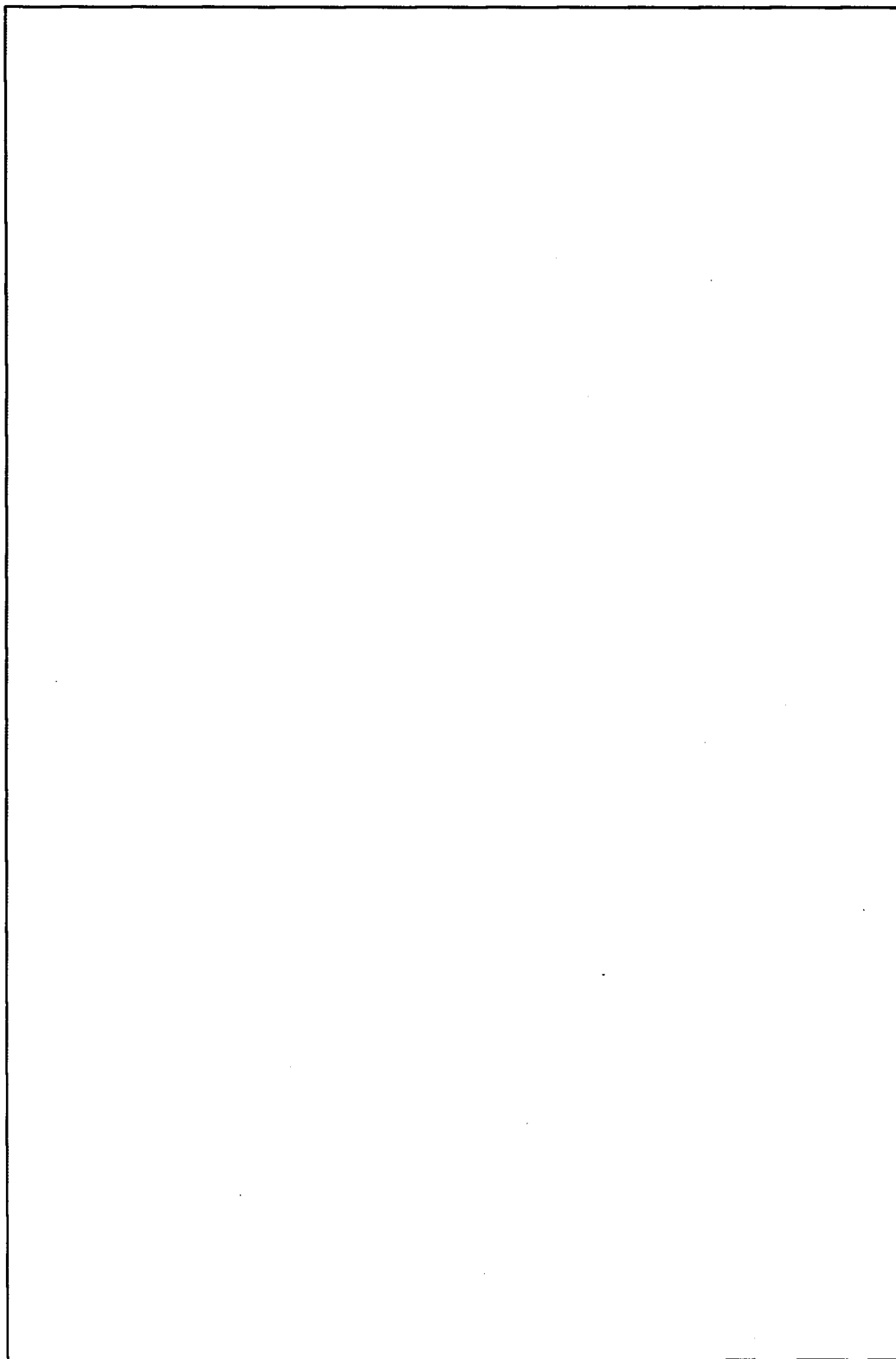
<u>ACRONYM</u>	<u>EXPANSION</u>
ACL	Accounting Legend Code
CA	Controlling Authority
CCI	Controlled Cryptographic Item
COMSEC	Communications Security
CT	Cipher Text
DAA	Designated Approving Authority
DTD	Data Transfer Device (AN/CYZ-10)
EIP	Embeddable INFOSEC Product
EKMS	Electronic Key Management System
HMI	Human/Machine Interface
HTTP	Hyper Text Transfer Protocol
KEK	Key Encryption Key
LA	Local Authority
PT	Plain Text
SA	Security Administrator
TEK	Traffic Encryption Key
VIP	ViaSat Internet Protocol

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

DISTRIBUTION:



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
