NSTISSI No. 3025
August 1999

(U) OPERATIONAL SECURITY DOCTRINE FOR CIPHERTAC 2000 (CTAC 2000)

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

National Security Telecommunications And Information Systems Security Committee

NSTISSC

NATIONAL MANAGER

FOREWORD

1. (U) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3025, "Operational Security Doctrine for the CipherTAC 2000 (CTAC 2000)," prescribes the minimum security standards for the protection and use of the CTAC 2000 handheld cellular encryption device.

2. (U) The CTAC 2000 is designed for use with the Motorola MicroTAC Elite™ cellular telephone. The CTAC 2000/MicroTAC Elite™ combination forms a lightweight, handheld STU-III (Type 1) compatible device. The procedures contained in this Instruction take into account the fact that the CTAC 2000 will be used in a variety of environments. Therefore, these procedures are designed so as not to inhibit use of the CTAC 2000.

3. (U) Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this NSTISSI 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~~) Comments and suggestions regarding this NSTISSI may be sent directly to the National Security Agency, [redacted]

Michael V. Hayden

MICHAEL V. HAYDEN
Lieutenant General, USAF

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

NSTISSC Secretariat [redacted] • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716
[redacted]

(U) OPERATIONAL SECURITY DOCTRINE FOR THE CIPHERTAC 2000 (CTAC 2000)

SECTION I - (U) PURPOSE AND SCOPE

1. (U) This doctrine contains minimum security standards for the protection and use of the CipherTAC 2000 (CTAC 2000) handheld cellular encryption device.

2. (U) The provisions of this doctrine apply to all departments and agencies of the U.S. Government and their contractors who handle, distribute, account for, store, or use the CTAC 2000.

3. (U//~~FOUO~~) [redacted]

SECTION II - (U) DEFINITIONS

4. (U) Definitions and acronyms contained in NSTISSI No. 4009 (Reference 30.a) apply to this doctrine.

SECTION III - (U) EQUIPMENT/SYSTEM DESCRIPTION/LEVEL OF USE

5. (U) The CTAC 2000 is designed for use with the Motorola MicroTAC Elite™ cellular telephone. The CTAC 2000/MicroTAC Elite™ combination forms a lightweight, handheld STU-III (Type 1) compatible device designed to provide users in mobile environments connectivity to desktop STU-IIIs in a voice (4.8 kbps) only mode. This device is compatible with the analog Advanced Mobile Phone System (AMPS) cellular network.

6. (U//~~FOUO~~) [redacted]

7. (U) The user activates the secure voice capability of the CTAC 2000 by entering a personal identification number (PIN). Paragraph 13 of this doctrine provides detailed information regarding the PIN.

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

8. (U) Provided appropriately classified keying material is used with the device, the CTAC 2000 is approved to protect information classified up to and including the SECRET level. The CTAC 2000 is <u>not</u> approved for the protection of TOP SECRET information.

9. (U) The CTAC 2000 does not have a Type 2 cryptographic mode and, therefore, is not compatible with STU-III (Type 2) equipment.

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

SECTION IV - (U) KEYING INFORMATION

10. (U) <u>Keying Scheme</u>. Each user representative who has key ordering authority shall provide all necessary information required to complete the CIPHERTAC Key Order Request(s) (see Encl. to this doctrine or call [redacted] and, via the automatic fax-back service, request document #2000). The user or the user representative then sends the appropriate CTAC 2000(s) along with the key order request(s) to the EKMS Central Facility (CF). Each CTAC 2000 will be filled with a STU-III operational key at the CF where the keys are produced. Each keyed CTAC 2000 is protected by a PIN that is also generated at the CF. The keyed CTAC 2000(s) shall then be shipped, separately from the PIN(s), to the user's COMSEC account as indicated on the key order request(s). When keyed CTAC 2000s are received at a user's COMSEC account, they may subsequently be handled and controlled in the same manner as other STU-IIIs held by that activity.

11. (U) The device can be filled with UNCLASSIFIED, CONFIDENTIAL, or SECRET STU-III key.

12. (U) The CF will automatically attach "mobile" to the key description code for keys that are loaded into CTAC 2000 devices.

U//~~FOUO~~

NOTE: (U) [redacted]

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

13. (U) <u>PIN Information</u>.

a. (U//~~FOUO~~) [redacted]

NOTE: (U//~~FOUO~~) [redacted]

(1) (U) A four digit PIN is assigned to devices filled with UNCLASSIFIED Key.

(2) (U) A seven digit PIN is assigned to devices filled with CONFIDENTIAL or SECRET Key.

NOTE: (U) In and of itself, the PIN is unclassified as long as it is not directly associated with a specific CTAC 2000 device.

b. (U) Since the CTAC 2000 does not have an over-the-air electronic rekey function, it is recommended that the user record and safeguard the PIN information to prevent unnecessary physical rekey operations.

c. (U) The PIN shall never be written on or otherwise affixed to the CTAC 2000.

d. (U) Activities holding multiple CTAC 2000 devices are authorized to generate listings of user PINs. The activity shall designate an appropriate security official(s) to maintain custody of this listing which should only be used when an authorized user forgets or otherwise loses their PIN. Such a listing shall be marked FOR OFFICIAL USE ONLY. However, under no circumstances shall these activities generate listings that associate a user's name and PIN with a specific CTAC 2000 device.

14. (U) Initial Keying and Rekeying Information.

a. (U) Initial keying and rekeying of the CTAC 2000 will require the user to send the device, along with a key order request, to the CF using one of the addresses shown below:

Mailing Address **FEDEX/overnight courier address**

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

[redacted]

NOTE: (U) FEDEX requires the name and telephone number of a person to be contacted at a recipient activity. Users should contact the EKMS Central Facility at (800) 635-5689 to obtain a name and current telephone number of an authorized recipient.

b. (U) The CTAC 2000 does not have over-the-air electronic rekey capability, and thus the CTAC 2000 **must always be rekeyed manually**.

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

NOTE: (U) Whenever notification is received, either through the display on the CTAC 2000 or by other means, that the key is due to expire, action should be taken to ensure the device is returned to the CF no later than two weeks prior to the scheduled expiration date.

d. (U) Anytime it becomes necessary to return a CTAC 2000 to the CF, users must be aware of the fact that **they will be without the device for a period of time ranging anywhere from 48 hours to several days**.

e. (U) If the CTAC 2000 contains key, it **must be zeroized** prior to shipping the device to the CF for rekey.

NOTE: (U) Procedures used to zeroize the CTAC 2000 are contained in the "CipherTAC 2000 Owner's Manual" which is provided by the manufacturer.

SECTION V - (U) CONTROL REQUIREMENTS

15. (U) NSTISSI No. 4001 (Reference 30.b) prescribes the minimum national standards for handling and control of unkeyed CCI equipment and components. These procedures also apply to a CTAC 2000 that satisfies the criteria set forth in paragraph 17.a, below. When the secure capability of the CTAC 2000 has been activated by entering the PIN, the device must be protected to the classification level of the key it contains. NSTISSI No. 4005 (Reference 30.c) prescribes the minimum national standards governing access to COMSEC material.

16. (U) Accounting Requirements. The CTAC 2000 is accountable by its serial number. When the CTAC 2000 is handled in the COMSEC Material Control System (CMCS), it shall be assigned Accounting Legend Code (ALC) 1.

NOTE: (U) The CTAC 2000 serial number shall be found on a label placed on the unit that indicates the "GSN: STUQ44" followed by a sequence of digits.

17. (U) Storage and Handling.

a. (U) So as not to overly inhibit its use, a keyed CTAC 2000 (one that has been loaded with key by the CF) may be handled the same as an unkeyed CTAC 2000 provided the PIN remains separate from the device.

b. (U) The user of a CTAC 2000 must maintain continuous physical control of the device or keep it stored in a manner that will minimize the possibility of loss or theft, unauthorized use, or tampering.

18. (U) Automatic Disabling Feature. The CTAC 2000 security features are protected with the PIN. The PIN allows ten limited attempts to unlock the security features. Further incorrect attempts will activate the automatic zeroization process.

NOTE: (U//~~FOUO~~) [redacted]

19. (U) Transportation. Because of certain unique characteristics of the CTAC 2000, approved procedures for the shipment of this device differ from procedures normally associated with either CCI devices in general or the STU-III in particular. Accordingly, the following guidance applies:

a. (U) CTAC 2000 devices, whether unkeyed (zeroized) or keyed, shall only be shipped by the authorized modes of transportation set forth in NSTISSI No. 4001 (Reference 30.b).

b. (U) The CTAC 2000 shall only be exported to those foreign governments to which release of the device has been approved by the National Manager.

c. (U) The CTAC 2000 may be shipped to authorized U.S. users at locations outside the continental United States.

d. (U) A U.S. user may carry a CTAC 2000 as an item of personal property to locations outside the United States, its territories and possessions provided its use is restricted to official purposes only.

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

20. (U) Procedures to Minimize Risk. To minimize the necessity for applying additional security restrictions, users should consider the following recommendations to reduce the level of risk:

a. (U) When talking at a classified level, be aware of environmental conditions, specifically the proximity of uncleared individuals. Although the CTAC 2000 can secure a telephone conversation, it cannot secure the surroundings.

b. (U) Keep the PIN and the CTAC 2000 separate.

c. (U) Use the CTAC 2000 only when no other secure means of communication are available.

SECTION VI - (U) MAINTENANCE

21. (U//~~FOUO~~) [redacted]

22. (U) Unless it is impossible to do so, all failed CTAC 2000 devices shall be zeroized prior to being shipped to the vendor for repair or replacement. If the device cannot be zeroized, it shall be handled consistent with the classification level of the key it holds. Procedures contained in NSTISSI No. 4005 (Reference 30.c)for transportation of keying material shall apply for shipment of such a device.

SECTION VII - (U) DISPOSITION/DESTRUCTION

23. (U//~~FOUO~~) [redacted]

24. (U//~~FOUO~~) [redacted]

25. (U) Excess and unserviceable CTAC 2000 devices must be zeroized by the user before they are shipped to another activity.

SECTION VIII - (U) REPORTABLE COMSEC INCIDENTS

26. (U//~~FOUO~~) [redacted]

a. (U) Evidence of possible tampering with, or unauthorized access to, a CTAC 2000.

b. (U) Loss or theft of a keyed CTAC 2000. I413 will report the loss or theft to the CF so the specific CTAC 2000 key can be added to the STU-III compromised key list (CKL).

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

27. (U) COMSEC incidents involving unkeyed (zeroized) CTAC 2000 devices shall be reported in accordance with procedures set forth in reference 30.b.

NOTE: (U) To submit a telephonic report of incident, contact [redacted]

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

28. (U) Any other incident that may constitute a violation of the procedures set forth in this doctrine shall be considered administrative in nature and shall be handled within department or agency channels.

SECTION IX - (U) EXCEPTIONS

29. (U//~~FOUO~~) [redacted]

SECTION X - (U) REFERENCES

30. (U) The following national-level documents are referenced in this doctrine.

a. (U) NSTISSI No. 4009 (Revision 1), National Information Systems Security (INFOSEC) Glossary, January 1999.

b. (U) NSTISSI No. 4001, Controlled Cryptographic Items, July 1996.

c. (U) NSTISSI No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 1997.

d. (U) NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, 2 December 1991.

Encl:
CIPHERTAC Key Order Request

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

DIF

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

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

DIF

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

DISTRIBUTION: [redacted]

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

[redacted]