NSTISSI No. 3006
August 2001

NSTISSC

(U) Operational Security Doctrine for the NAVSTAR Global Positioning System (GPS) Precise Positioning Service (PPS) User Segment Equipment

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

NSTISSI No. 3006

NSTISSC

National Manager

FOREWORD

1. (U) This National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3006 establishes the minimum national security standards for the handling and control of the NAVSTAR Global Positioning System (GPS) Precise Positioning Service (PPS) User Segment Equipment, its components, and associated key.

2. (U) This instruction consolidates and supersedes NTISSI No. 3006, *Operational Security Doctrine for the NAVSTAR Global Position System (GPS) User Segment*, dated 28 June 1988 and NAG-54, *Operational Security Doctrine for NAVSTAR Global Positioning System User Segment*, dated May 1996.

3. (U) Comments and suggestions regarding this NSTISSI may be directed to the NSA [redacted]

4. (U) Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction from the Secretariat at the address listed below.

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

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

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

(U) OPERATIONAL SECURITY DOCTRINE FOR NAVSTAR GLOBAL POSITIONING SYSTEM (GPS) PRECISE POSITIONING SERVICE (PPS) USER SEGMENT EQUIPMENT

TITLE SECTION

SECTION I - (U) INTRODUCTION

1. (U) Purpose - This doctrine contains minimum security standards for the protection and use of the NAVSTAR GPS PPS User Segment Equipment and associated communications security (COMSEC) material.

2. (U) Application - The provisions of this doctrine apply to departments and agencies of the U.S. Government and their contractors who use the NAVSTAR GPS PPS User Segment Equipment and associated COMSEC material.

3. (U) Promulgation - Departments and agencies of the Federal Government are obligated to disseminate the information in this document to their subordinate elements and contractors who use the GPS PPS User Segment Equipment. Promulgation may be effected by issuing this document or by incorporating its contents in department/agency publications.

4. (U) Foreign Release

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

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

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

[redacted]

NOTE: (U) The NSA International Relations Division may be reached at [redacted]

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

6. (U) References – References cited in this instruction are listed in ANNEX A.

7. (U) Definitions - For reader convenience, selected definitions from the NSTISSI No. 4009. (Reference d) and FED-STD-1037C, along with system-unique specialized terms used in this instruction are defined in ANNEX B.

8. (U) Acronyms – Acronyms used in this instruction are expanded with first use and are listed in ANNEX C.

9. (U) Relationship to General Doctrine - ANNEX D lists general doctrine applicable to the COMSEC material associated with the GPS PPS.

10. (U//~~FOUO~~) Conflicts with Other Documents - Any conflicts between this doctrine and other published national-level doctrine should be brought to the attention of the National Manager for NSTISSC. However, this does not preclude any department or agency of the U.S. Government from applying more stringent security measures to their equipment than this doctrine requires.

SECTION II - (U) SYSTEM DESCRIPTION

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

12. (U) Services – The GPS provides two levels of service, Standard Positioning Service (SPS) and Precise Positioning Service (PPS).

a. (U) SPS - The SPS is a positioning and timing service that is available to all GPS users. It is intended primarily for civil use. Access to the SPS is openly available and does not require the use of cryptography.

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

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

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

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

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

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

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

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

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

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

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

SECTION III - (U) KEYING

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

NOTE: (U) The GPS CA can be reached at [redacted]

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

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

17. (U) Types of GPS Key - There are several types of key available to authorized PPS users. These are differentiated by their application (i.e., operational, maintenance, and simulator test), by their nature (i.e., Group-Unique Variable (GUV) Key Encryption Key (KEK), BLACK GUV (BGUV) KEK, BLACK Cryptovariable monthly (BCVm) Key Production Key (KPK), or Cryptovariable weekly (CVw) KPK), and by their format (i.e., electronic, punched paper tape, or printed keylist). The GPS keys are identifiable by their CMCS long and short titles.

a. (U) Operational Keys allow HAE to access the PPS.

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

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

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

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

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

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

[redacted]

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

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

NOTE: (U) Cryptoperiods for these types of GPS keys are subject to change or irregular supersession by the CA.

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

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

(1) (U~~//FOUO~~) [redacted]

(2) (U~~//FOUO~~) [redacted]

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

19. (U) Key Loading - GPS key loading may be accomplished with NSA-approved fill devices, such as the KOI-18 general purpose tape reader, the KYK-13 electronic transfer device, the AN/CYZ-10 Data Transfer Device (DTD), or with an NSA-approved GPS key loader.

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

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

[redacted]

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

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

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

NOTE: (U) The NSA GPO may be reached at [redacted]

NOTE: (U) GPS BLACK keys and BLACK Update Parameters will not be recognized by the KYK-13 nor DTD. As a result, the KYK-13 light will not flash when the BLACK keys or update parameters are loaded. Also, when the keys are loaded into a DTD from a KOI-18, the DTD may request that the tape be pulled through the KOI-18 a second time.

20. (U) Key Destruction

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

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

SECTION IV - (U) PHYSICAL SECURITY

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

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

[redacted]

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

[redacted]

(1) (U//~~FOUO~~)

[redacted]

(2) (U//~~FOUO~~)

[redacted]

(3) (U//~~FOUO~~)

[redacted]

(4) (U//~~FOUO~~)

[redacted]

(5) (U//~~FOUO~~)

[redacted]

(6) (U//~~FOUO~~)

[redacted]

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

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

(7) (U//~~FOUO~~) [redacted]

(8) (U//~~FOUO~~) [redacted]

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

(U) PPS USER EQUIPMENT CLASSIFICATION

[redacted]

c. (U) Zeroization and Key Storage

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

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

(4) (U//~~FOUO~~) [redacted]

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

[redacted]

22. (U) Accountability and Handling

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

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

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

d. (U) Inventories - Within each organization, inventories of the GPS equipment must be accomplished at least annually and whenever there is a change of personnel responsible for the safekeeping or accounting of an organization's holding of the PPS equipment and components. Discrepancies must be reported in accordance with paragraph 28.

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

f. (U) Safeguarding Key - Except as indicated in SECTION V, the GPS key must be accounted for in the CMCS, in accordance with NSTISSI No. 4005.

23. (U) Maintenance - Maintenance of PPS HAE may be performed only by appropriately cleared U.S. citizens or U.S. resident aliens who are employees of the U.S. Government. Any deviation from this policy must be approved by the NSA GPO, on a case-by-case basis. A SECRET security clearance is required for maintenance personnel who have access to the GPS cryptographic design information and classified GPS interface control documents.

24. (U) Shipment - Unkeyed PPS HAE must be zeroized prior to shipment and must be shipped by means approved for the transportation of Government property. Shipment of

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

equipment in a keyed state is permissible if mission requirements dictate or if the equipment cannot be zeroized due to malfunction. Keyed, classified PPS HAE may be shipped to users in accordance with NSTISSI No. 4005. UNCLASSIFIED PPS HAE may be shipped as sensitive but UNCLASSIFIED equipment (e.g., by U.S. Registered Mail) where a receipting system and a means for tracer action is available if the equipment is presumed lost or misrouted. SECRET PPS-capable GPS simulators must be shipped in accordance with service and NISPOM requirements for SECRET hardware and software. Loss of keyed PPS HAE must be reported to the GPS CA as a COMSEC incident.

> **NOTE:** (U) Prior to the shipment of keyed PPS HAE, approval must be obtained from the GPS CA.

25. [redacted]

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

27. (U) Destruction

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

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

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

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

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

c. **(U) Emergencies - The safeguarding of COMSEC key under emergency conditions is the responsibility of each holder and should be included in the holder's Emergency Action Plan, if such a plan is required for the using site.**

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

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

SECTION V - (U) NON-STANDARD GPS KEY HANDLING

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

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

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

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

[redacted]

30. (U) Programs in the GPS User Segment

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

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

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

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

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

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

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

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

f. (U) Interface Devices - Equipment used to provide key loading capability for the GPS receivers, through means other than standard key fill ports and that does not fall into any of the categories mentioned above.

NOTE: (U) Interface devices may be as simple as a direct electrical connection through a multi-function box or as complex as a ruggedized portable computer.

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

31. (U) Key Handling Principles - Once loaded onto an AIS, the GPS keys can no longer be accounted for within CMCS, thus the "CRYPTO" handling caveat is removed. The GPS RED keys must be handled as SECRET data and the GPS BLACK keys must be handled as sensitive but UNCLASSIFIED data. Adaptations of standard INFOSEC requirements to the special case of GPS key handling are addressed below:

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

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

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

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

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

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

32. (U) Key Handling Requirements

a. (U) Cryptographic CONOP - Each system approved under this SECTION must provide a GPS cryptographic CONOP, either as an appendix to a system-level CONOP document or as a separate document.

(1) (U) Included Data - In general, only program/system data directly pertinent to the GPS cryptographic functions should be included in a GPS Cryptographic CONOP document. Peripheral program/system data should be appropriately referenced. Specifically, items addressing the means by which key is delivered to the servicing COMSEC account is not required.

NOTE: (U) GPS CONOP submitters may assume that the approval authority has the technical expertise to review basic schematics and flow charts.

(2) (U) User Manuals - The cryptographic CONOP documents a program's security measures and is not necessarily part of the program's user manuals.

(3) (U) Root Documents - If a cryptographic CONOP involves a dependent module that interfaces to a separately approved system (e.g., the module that supports a specific airframe on a MPS), the root document should be referenced rather than incorporated. Alternatively, several cryptographic CONOPs covering portions of a key transfer path could be combined into a single cryptographic CONOP covering the MPS module for a specific airframe and the handling of key on that aircraft.

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

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

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

(b) (U//~~FOUO~~) [redacted]

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

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

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

(1) (U~~//FOUO~~) [redacted]

(2) (U) Nonvolatile Storage

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

(b) (U~~//FOUO~~) [redacted]

1. (U) The system enforces discretionary access controls;

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

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

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

(4) (U~~//FOUO~~) [redacted]

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

[redacted]

(1) (U//~~FOUO~~) [redacted]

NOTE: (U) For the GPS BLACK keys, audit trails may remain UNCLASSIFIED//FOR OFFICIAL USE ONLY (exempt from mandatory disclosure under the Freedom of Information Act, Exemption 3 applies) if the key edition is not related to the key's effective period. If a key's effective period is associated with the key edition, the audit trail becomes CONFIDENTIAL.

(2) (U//~~FOUO~~) [redacted]

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

(4) (U//~~FOUO~~) [redacted]

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

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

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

(1) (U//~~FOUO~~) [redacted]

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

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

(b) (U~~//FOUO)~~ [redacted]

(2) (U) [redacted]

NOTE: (U) [redacted]

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

(b) (U~~//FOUO)~~ [redacted]

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

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

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

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

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

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

(b) (U//~~FOUO~~) [redacted]

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

(d) (U//~~FOUO~~) [redacted]

g. <u>(U) Handling GPS Key in External Media, Data Bases, and Network Connections</u>

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

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

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

(4) (U//~~FOUO~~) [redacted]

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

(b) (U//~~FOUO~~) [redacted]

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

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

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

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

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

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

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

SECTION VI - (U) CRYPTOGRAPHIC CONOP

33. (U) Cryptographic CONOP FORMAT - Listed in ANNEX E are the basic sections of each cryptographic CONOP, with a short description of the data covered in each section:

NOTE: (U) Cryptographic CONOP documents have no specified minimum or maximum length, other than that necessary to contain all appropriate data. All

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

GPS CONOP documents are at a minimum UNCLASSIFIED//FOR OFFICIAL USE ONLY.

SECTION VII - (U) NONVOLATILE MEDIA STATEMENTS

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

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

a. (U) Permanent Classification Statement

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

b. (U) The following additional information is provided:

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

35. (U) GPS BLACK Key CRYPTO Statement

a. (U) The GPS CRYPTO statement expressed below must be applied to all nonvolatile media used to record or transfer the GPS BLACK key.

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

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

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

[redacted]

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

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

ANNEXES:

A - References
B - Definitions
C - Acronyms
D - Doctrine Relationship
E - Sample CONOP

ANNEX A

(U) REFERENCES

a. NSTISSP No. 8, National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Foreign Governments, dated 13 February 1997

b. CJCSI 6510.01b, Defensive Information Operations Implementation, dated 26 August 1998

c. Department of Defense Global Positioning System (GPS) Security Policy, dated 29 March 1999

d. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated September 2000

e. NSTISSP No. 4, National Policy on Electronic Keying, dated November 1992

f. NSTISSI No. 4005, Safeguarding COMSEC Facilities and Material, dated August 1997

g. National Industrial Security Program Operating Manual (NISPOM), dated January 1995

h. NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987

i. NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991

j. DoD 5200.1-R, Information Security Program, dated 17 January 1997

k. NAVSTAR Global Positioning System System Protection Guide, dated 13 June 1997

ANNEX B

(U) DEFINITIONS

(U) For reader convenience, selected definitions from NSTISSI 4009 are quoted below, along with definitions for system unique, specialized terms used in this instruction.

NOTE: (U) Notes following some definitions contain elaborative information and are not included in the associated definitions.

a. (U) BLACK Key - Key that is protected by encryption with a key encryption key and that must be decrypted before it can be used. (System Unique)

NOTE: (U) A GPS TEK that is available in a satellite downlink is an example of a BLACK key. Although it is not available through conventional key distribution, a SAASM makes use of the GPS BLACK keys.

b. (U) BLACK Cryptovariable Monthly (BCVm) - Key production key used to autonomously generate the TEKs within each GPS user equipment. (System Unique)

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

NOTE: (U) In contemporary U.S. COMSEC application, the term "key" has replaced the term "cryptovariable;" however, it is impractical to implement this change fully with respect to the GPS PPS Program.

c. (U) BLACK Update Parameter (BBKAUPD) - Information required by SAASM to decrypt the GPS BLACK keys. (System Unique)

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

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

d. (U) 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. Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI." (NSTISSI No. 4009)

e. (U) CRYPTO - Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information. (NSTISSI No. 4009)

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

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

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

g. (U) Dedicated Mode – Information system (IS) security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: (a) valid security clearance for all information within the system; (b) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs); and (c) valid need-to-know for all information contained within the IS. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. (NSTISSI No. 4009)

h. (U) Fill Device - COMSEC item used to transfer or store key in electronic form or to insert key into a crypto-equipment. (NSTISSI No. 4009)

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

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

j. (U) INFOSEC Boundary - Conceptual boundary that includes all GPS information systems security related functions. (System Unique)

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

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

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

l. (U) Key Administration - Functions of loading, storing, copying, and distributing the keys and producing the necessary audit information to support those functions. (System Unique)

m. (U) Key Encryption Key (KEK) - Key that encrypts or decrypts other key for transmission or storage. (NSTISSI No. 4009)

n. (U) Key Production Key (KPK) - Key used to initialize a keystream generator for the production of other electronically generated key. (NSTISSI No. 4009)

o. (U) Need-to-Know - Necessity for access to, or knowledge or possession of, specific information required to carry out official duties. (NSTISSI No. 4009)

p. (U) Nonvolatile Media - Devices that, once written, provide stable storage of information without external power supplies. (System Unique)

NOTE: (U) Examples of nonvolatile media are magnetic and optical media and some forms of silicon memory.

q. (U) Permanent Storage - Nonvolatile media that can never be completely erased once written.

NOTE: (U) Examples of permanent storage are magnetic media, WORM drives, and CDs.

r. (U) Precise Positioning Service (PPS) Host Application Equipment (HAE) - Generic term for devices that receive and process the PPS signals transmitted from a GPS satellite.

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

s. (U) RED Key - Key that is usable in its present form without any additional decryption. (System Unique)

t. (U) System High Mode - Information system (IS) security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: (a) valid security clearance for all information within an IS; (b) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs); and (c) valid need-to-know for some information contained within the IS. (NSTISSI No. 4009)

u. (U) Temporary Storage - Storage of the GPS keys in fully volatile memory, static random access memory, or electronically-erasable programmable read-only memory. (System Unique)

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

NOTE: (U) Examples of a fully volatile memory are a DRAM and derivatives.

v. (U) TEMPEST - Short term referring to the investigation, study, and control of compromising emanations. (NSTISSI No. 4009)

w. (U) Traffic Encryption Key - Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text. (NSTISSI No. 4009)

x. (U) Volatile Media - Devices that require external power supplies to maintain stored information.

ANNEX C

(U) ACRONYMS

AIS	Automated Information System
AOC	Auxiliary Output Chip
A-S	Anti-spoof
BBKAUPD	BLACK Update Parameter
BCVm	BLACK Cryptovariable Monthly
BGUV	BLACK Group-Unique Cryptovariable
CA	Controlling Authority
CCI	Controlled Cryptographic Item
CD	Compact Disc
CMCS	Communications Security Material Control System
COMSEC	Communications Security
CONOP	Concept of Operation
CVw	Cryptovariable Weekly
DAA	Designated Approving Authority
DoD	Department of Defense
DRAM	Dynamic Random Access Memory
DTD	Data Transfer Device (AN/CYZ-10)
EEPROM	Electrically Erasable Programmable Read Only Memory
EPROM	Erasable Programmable Read Only Memory
EKMS	Electronic Key Management System
FCS	Fire Control System

GPO	Global Positioning System Program Office
GPS	Global Positioning System
GUV	Group-Unique Variable
HAE	Host Application Equipment
INFOSEC	Information Systems Security
ISSO	Information Systems Security Officer
JPO	Joint Program Office (for GPS)
KDP	Key Data Processor
KEK	Key Encryption Key
KLIF	Key Data Processor Loading and Installation Facility
KPK	Key Production Key
MPS	Mission Planning System
NATO	North Atlantic Treaty Organization
NISPOM	National Industrial Security Operating Manual
NSA	National Security Agency
PPS	Precise Positioning Service
PPS/SM	Precise Positioning Service Security Module
RF	Radio Frequency
SA	Selective Availability
SA/A-S	Selective Availability/Anti-spoofing
SAASM	Selective Availability/Anti-Spoofing Module
SPS	Standard Positioning Service
SRAM	Static Random Access Memory
SSS	Satellite Signal Simulator

TEK	Traffic Encryption Key
USSPACECOM	United States Space Command
WORM	Write Once - Read Many

ANNEX D

(U) Relationship to General Doctrine

a. **(U) NSTISSI No. 4000** establishes minimum standards, delineates responsibilities, and establishes procedures for COMSEC equipment maintenance and maintenance training.

b. **(U) NSTISSI No. 4001** sets forth minimum requirements for controlling unkeyed controlled cryptographic item (CCI) equipment and components.

c. **(U) NSTISSI No. 4002** provides general guidance relative to the classification of COMSEC information.

d. **(U) NSTISSI No. 4003** contains a general listing of reportable COMSEC incidents and standards for reporting them.

e. **(U) NTISSI No. 4004** prescribes standards for routine destruction of COMSEC material and provides criteria and guidance for protecting COMSEC material under emergency conditions. It also provides guidance and assigns responsibilities for recovery of abandoned COMSEC material.

f. **(U) NSTISSI No. 4005** states the minimum standards for safeguarding and controlling keying material and establishes additional controls that apply when CCI (and/or classified) equipment is keyed.

g. **(U) NSTISSI No. 4006** describes responsibilities of organizations that serve as controlling authorities (CAs) for key and provides guidance for accomplishing those responsibilities.

h. **(U) NSTISSI No. 7000** establishes guidelines, restrictions, and procedures for determining the applicable TEMPEST countermeasures for equipment, systems, and facilities that process national security information.

i. **(U) Department of Defense Global Positioning System Security Policy** provides guidance on GPS security related to the operation, development, acquisition, and use of GPS User Equipment.

j. **(U) NAVSTAR Global Positioning System System Protection Guide** provides guidance on the protection of information, technologies, or systems which includes information or data which reveal the mission and characteristics of the GPS.

k. **(U) DoD 5200.1.R** implements Executive Order 12958, Classified National Security Information, and associated OMB directives within the Department of Defense.

ANNEX E

(U) SAMPLE CRYPTOGRAPHIC CONOP

(U) Cover Page - Include the issue date and a point of contact, such as the program office, for the CONOP.

(U) Table of Contents - List the SECTIONs and any appendices that are part of the CONOP.

(U) Introduction

1. (U) Overview - Give a top-level description of the overall employment of the system, including general information about its purpose and of the CONOP document. State whether or not it is an update of a previously-approved CONOP.

2. (U) Applicable Security Documents - Reference all security documents used in writing the CONOP, including appropriate national, DoD, and service doctrines and policies, as well as program-specific documents, such as the AIS accreditation document.

3. (U) Acronyms and Definitions - Provide definitions or explanations for program-specific terms and abbreviations.

(U) System Details

4. (U) System Description - Provide a description of the system, including identification of potential users and possible employment locations. Also address current or planned accreditation level (e.g., "operates at SECRET system-high level.")

5. (U) System Architecture - Describe hardware and operating system configurations. Cover memory types or other key storage media on the system, special architecture features that isolate the GPS keys, internal interfaces, and existing or planned external interfaces.

6. (U) Updates - Address the planned frequency of cryptographic CONOP updates, to incorporate security patches or other new requirements into the basic approved system and the method of ensuring that the new system meets all existing requirements.

(U) Administration and Use of GPS Keys

7. (U) Receipt of Keys - Address planned methods for introducing the keys into the system, including current loading methods and future methods, if a transition from punched tape to electronic key is planned.

8. (U) Handling and Auditing Keys - Address the number and type of keys that may simultaneously be present on the system and the locations used to store the keys. Also address methods of auditing all events related to the GPS key handling and reporting/reduction of the key handling audits.

9. (U) Key Applications - Address the programs or functions that manipulate the GPS keys. Specifically address capabilities that could lead to the display of the key to users not possessing the appropriate clearance, a need-to-know, and a COMSEC briefing, or that could cause output of the key to hardcopy.

10. (U) Key Transfers - Address any external interfaces or media to which the GPS key may be intentionally transferred. This may include reference to a separate CONOP document covering the receiving system.

11. (U) Key Destruction and Zeroization - Address the methods for ensuring that intermediate storage locations are properly zeroized and that the path of the key flow is fully traceable. Include information as to whether these functions are performed automatically and what users or roles can perform them manually. If the system is authorized for interim storage of the key, address the methods by which the key may be destroyed upon supersession or expiration.

12. (U) Compromise Recovery - Address planned actions to recover from potential key compromises and other unplanned events affecting the GPS key. Specifically address the following:

a. (U) Identification, labeling, and handling of inadvertent printed output or other output of the key to improper media.

b. (U) Planned actions during failure of the system to zeroize/destroy the key.

c. (U) Planned actions during and following abnormal power termination or machine exception state.

d. (U) Planned actions during a confirmed or suspected compromise of the GPS key.

e. (U) System features that would be used to protect the key in the event of an emergency destruction order or natural disaster.

13. (U) Foreign Releasability.

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

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

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

DISTRIBUTION:

[redacted]

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

[redacted]

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