NSTISSAM - COMSEC/1-93
14 October 1993

NOMENCLATURE

FOR

COMMUNICATIONS SECURITY MATERIAL (U)

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

~~FOR OFFICIAL USE ONLY~~

NSTISS
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

NATIONAL MANAGER

14 October 1993

FOREWORD

1. National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) COMSEC/1-93, "Nomenclature for Communications Security Material," describes the nomenclature assigned to U.S., allied, and NATO communications security (COMSEC) material. This NSTISSAM supersedes NACSIM No. 2002, COMSEC Nomenclature System, dated 30 December 1982.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this advisory memorandum from:

Executive Secretariat
National Security Telecommunications and Information Systems Security Committee
National Security Agency
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

3. U.S. Government contractors are to contact their appropriate government agency or Contracting Officers Representative regarding distribution of this document.

J. M. McCONNELL
Vice Admiral, U. S. Navy

NOMENCLATURE FOR COMMUNICATIONS SECURITY MATERIAL

SECTION I - PURPOSE AND SCOPE

1. This document explains the nomenclature assigned to U.S., allied, and NATO communications security (COMSEC) material. The information contained in this NSTISSAM should be made available to all U.S. Government departments and agencies, and their agents, who hold or use COMSEC material.

SECTION II - REFERENCES

2. This NSTISSAM refers to the following documents.

a. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992.

b. MIL-STD-196D, Military Standard, Joint Electronics Type Designation System, dated 19 January 1985.

SECTION III - DEFINITIONS

3. The definitions published in NSTISSI No. 4009 apply to this NSTISSAM. For the purpose of this document, the following definitions are also applicable:

a. Authentication Equipment. Equipment designed to provide protection against fraudulent transmissions and imitative communications deception or to establish the authenticity of a transmission, message, station, originator, or telecommunications system.

b. COMSEC Equipment System. A grouping of COMSEC equipment that, of itself, provides communications security for a particular communications link, end-to-end switched communication path, terminal, or switching center.

c. Nonflight Satellite Production Equipment. A model that is representative of high-reliability production models in form, fit, and function, but is not suitable for use in the operational satellite. It does not provide the high reliability of a production model due to extra testing, choice of lower reliability parts, or potential of unverified mechanisms.

SECTION IV - DISCUSSION

4. Types of Nomenclature.

a. COMSEC hardware can be assigned nomenclature from a number of sources. Either of two formal systems--the National Security Agency (NSA) Telecommunications Security (TSEC) nomenclature system or the DoD Joint Electronic Type Designation System (JETDS)--can be used. COMSEC nomenclature taken from these systems is usually referred to as a short title. In addition, many commercially developed cryptographic and telecommunications and information handling equipment are not assigned traditional nomenclature, but will bear the manufacturer's commercial designator (e.g., STU-III, Wang TIU, XEU).

b. COMSEC firmware, hard copy keying material, and electronic key management system (EKMS) keying material are assigned nomenclature from the TSEC nomenclature system only. Key generated locally under the provisions of NAG-16 (Field Generation and Distribution of Electronic Key, available from NSA) is not assigned a short title, but is assigned an identification tag by the producer for record keeping purposes.

c. COMSEC aids that are controlled outside of the COMSEC material control system (CMCS) will be assigned nomenclature as determined appropriate by the originator. For example, certain limited maintenance manuals are assigned the designator LMM (LMM-1, LMM-2).

5. NSA Task Title. During the early stages of the development cycles of NSA-developed COMSEC equipment, task titles (e.g., VINSON, THORNTON) are assigned for convenience in differentiating the various evolving programs. After

nomenclature is assigned and until the equipment goes into production, NSA task titles are normally shown in correspondence in parentheses. Although these task titles are officially dropped from correspondence when an equipment enters its first production contract, they sometimes continue in colloquial use as system designators.

SECTION V - TSEC NOMENCLATURE

6. Description. The TSEC nomenclature system was devised to designate COMSEC hardware and hard copy keying material, as well as certain documents that the United States employs for its own use and for use with its allies. TSEC nomenclature is assigned to all hard copy keying material and COMSEC firmware; however, in recent years its use on hardware has diminished in favor of JETDS nomenclature. TSEC nomenclature is not assigned to COMSEC-related documents, such as Technical Information Bulletins (TIBs) and Communications Security Equipment Systems Documents (CSESDs), interconnecting boards, extender boards, board extractors, mounting bases, interconnecting cables, repair and spare parts containers, carrying cases, control panels, and most adapter units, or to commercial items. Since NSA is responsible for producing or authorizing the production of all COMSEC hardware and hard copy key used by the U.S. Government to secure national security systems, only NSA is authorized to assign TSEC nomenclature to that type of material. Electronic keying material, produced within EKMS by NSA-approved key generation elements and distributed throughout EKMS, will be assigned TSEC nomenclature by those generating elements.

7. Assignment. TSEC nomenclature may be assigned to COMSEC equipment as soon as the decision to develop it for user evaluation has been made. Assembly, subassembly, and element designators are assigned upon identification of the equipment's internal configuration. TSEC nomenclature is assigned to hard copy COMSEC aids immediately upon receipt of request for production. Within the EKMS, TSEC nomenclature is assigned upon receipt of a request for short title.

8. Equipment Short Titles. The short titles assigned to COMSEC equipment are comprised of the following elements, in the order shown:

a. The nomenclature system designator "TSEC" followed by a slant (/). The TSEC prefix may be deleted from the short title when an equipment or component is designated Controlled Cryptographic Item (CCI).

b. A descriptive digraph followed by a dash. Descriptive digraphs are selected from ANNEX A and consist of a function designator to show the basic function of the equipment and a type designator to show the general type of the equipment.

c. A unique item number. In correspondence and technical documentation (never on nameplate), a TSEC short title may be followed by unfilled parentheses to denote a series or line of equipment models, e.g., TSEC/KG-83().

d. A model designator, when appropriate. Model designators--Exploratory Development (X), Advanced Development (V), Engineering Development (E), and Preproduction (P)--are employed to designate COMSEC equipment at the various evolutionary stages in the development cycle (e.g., the nomenclature "TSEC/KG-83 (P-1)" designates the first pre-production model of the KG-83 equipment). With the exception of nonflight satellite production equipment, which is designated by the letter N, model designators are not assigned to production models of COMSEC equipment.

9. Assembly Short Titles. The short titles assigned to COMSEC assemblies are comprised of the following elements, in the order shown.

a. A descriptive trigraph, selected from ANNEX A, followed by a dash. Trigraphs indicate the function and type designators of the equipment for which the assembly is a part and the specific function performed by the assembly. Assembly numbers are assigned to correspond, where possible, to the number of the equipment with which the assembly is used (e.g., KG-66, KGV-66, KGR-66). In circumstances where equipment contains more than one assembly, functionally similar but not interchangeable, each assembly designator is distinguished by a sequentially assigned number preceded by a dash (e.g., HNT-10-1/TSEC, HNT-10-2/TSEC).

b. A unique item number.

c. A model designator, when appropriate (see 8.d., above).

d. The nomenclature system designator "TSEC" preceded by a slant (/). (The TSEC prefix may be deleted from the short title when an equipment or component is designated CCI.)

10. Subassembly Short Titles. The designator assigned to COMSEC subassemblies is comprised of the following elements, in the order shown below. The nomenclature designator "TSEC" is not used in subassembly, element, and classified microcircuit short titles.

a. The letter "Z" followed by a dash.

b. A unique alphabetic trigraph that begins with "AAA" and continues through "ZZZ."

11. Element Designators. COMSEC elements include microcircuit boards and printed circuit boards. The designator assigned to COMSEC elements is comprised of the following elements, in the order shown:

a. The letter "E" followed by a dash.

b. A unique alphabetic trigraph that begins with "AAA" and continues through "ZZZ."

12. Microcircuit Chip Designators. The designators assigned to microcircuit chips are comprised of the following elements in the order shown:

a. The letter "U" followed by a dash.

b. A unique alphabetic trigraph that begins with "AAA" and continues through "ZZZ."

13. COMSEC Equipment System Short Titles. COMSEC equipment system designators are used to identify a group of equipment that functions together. They may be used in correspondence or technical documentation, but do not appear on equipment nameplates. The short titles assigned to COMSEC equipment systems are comprised of the following elements in the order shown:

a. The nomenclature system designator "TSEC" followed by a slant (/).

b. A descriptive digraph followed by a dash. The descriptive digraph is selected from ANNEX A and includes the letter "C" as the function designator and a type designator to show the general type of the system. Variations of a basic COMSEC equipment system are identified by a suffix, consisting of a dash and a number (e.g., TSEC/CY-2-1 is the Narrowband Secure Voice System-Ground Terminal).

c. An item number.

14. Modification Designators.

a. Each major modification to a production model of COMSEC equipment or assembly, or applicable software, is identified by the addition of a modification suffix letter to the short title (e.g., TSEC/KG-43 to TSEC/KG-43A). A major modification is one that results in loss of inter-changeability of component parts between the modified and unmodified versions, but not loss of the ability to maintain cryptographic compatibility.

b. Each minor modification made to an equipment or assembly is identified by an appropriate marking on the modification record plate affixed to the modified equipment or assembly, or by the appropriate modification number placed on the modified equipment or assembly. The short title of the modified equipment is unchanged. A minor modification is one that affects neither cryptographic compatibility nor physical interchangeability. NSA is responsible for the acquisition and distribution of nameplates required as a result of modification, redesignation, or reclassification of all U.S.-produced COMSEC equipment used to secure national security systems.

c. Repair actions made to an equipment or assembly are not identified by any marking, but are fully documented by maintenance manual changes.

d. Minor modifications of subassemblies or elements, that affect neither cryptographic compatibility nor physical interchangeability, are identified by a modification number preceded by a slant, e.g., Z-ACC/1.

e. When subassemblies or elements are modified to the extent that either physical interchangeability or cryptographic compatibility is lost, a new trigraph is assigned to the modified subassembly or element.

f. Changes of equipment, within a COMSEC equipment system, do not necessarily change the system designator.

g. Short titles of COMSEC aids normally are not amended and will not be amended to show changes in classification, copy count, number of holders, relationship to another short title, intended usage, or modification status.

15. Keying Material. NSA produces the types of keying material listed below. Key may be unclassified or classified at the level of the information it is intended to protect.

a. Exercise Key. Key intended to safeguard transmissions associated with exercises. It is used on-the-air, is marked CRYPTO, and bears the release prefix "US" or "A."

b. Maintenance Key. Key intended only for off-the-air, in-shop use. It is not marked CRYPTO, and bears no release prefix.

c. Operational Key. Key intended for use on-the-air for protection of operational information or for the production or secure electrical transmission of key streams. It is marked CRYPTO, and bears the release prefix "US" or "A."

d. Sample Key. Key intended for off-the-air demonstration use only. It is not marked CRYPTO and bears no release prefix.

e. Test Key. Key intended for on-the-air testing of COMSEC equipment or systems. It is marked CRYPTO, and bears the release prefix of "US" or "A."

f. Training Key. Key intended for on-the-air or off-the-air training. If it is used for on-the-air training, it is marked CRYPTO, and bears the release prefix "US" or "A." If it is used for off-the-air training, it is not marked CRYPTO and bears no release prefix.

16. Keying Material Short Titles. This includes keying material produced in the form of integrated circuit devices such as programable read only memories (PROMs) and large scale integrated circuits (LSIs). Short titles assigned to COMSEC keying materials are comprised of the following elements, in the order shown:

a. The release prefix "US" or "A" if marked CRYPTO. The release prefix "US" is assigned to key reserved exclusively for U.S. use. The release prefix "A" is assigned to key that is shared by the U.S. and specified allies.

b. The functional relationship, purpose, and type aid designators selected from ANNEX B. (The purpose designator "E" is used only for key that remains encrypted from the point of generation through receipt by the using equipment.)

c. An item number preceded by one character space, (e.g., USKAT 123 or USKAT A123).

d. Within EKMS, short titles will also include the six-digit EKMS identifier of the generating element. The EKMS identifier is placed after the item number and is usually the COMSEC account number of the generating element (e.g., USEAD 123 888888).

e. An edition letter or number preceded by one character space. Edition letters are assigned to general documents and to regularly superseded keying materials, beginning with "A," and proceeding sequentially through "ZZZZZZ." Edition designators for some irregularly superseded keying materials begin with "1" and ascend sequentially through "999999."

f. Part designators, when appropriate. Certain types of critically sensitive keying material are produced and handled in two parts, identified as "PART A" and "PART B," (e.g., USKAZ 100 PART A, Edition G).

17. Short Titles for COMSEC Manuals. Short titles for general, operating, and maintenance documents that are controlled within the CMCS are comprised of the following elements, in the order shown:

a. Functional relationship, purpose, and type aid designators selected from ANNEX B.

b. An item number preceded by a dash.

c. An edition letter.

d. The nomenclature system designator "TSEC" preceded by a slant (/).

SECTION VI - JETDS NOMENCLATURE

18. Description. JETDS nomenclature is assigned to electronic material that is used by the Department of Defense and is employed in the fields of data processing, detection and tracking, recognition and identification, communications, aids to navigation, weapons control and evaluation, flight control, and electronics countermeasures. The material may be classified or unclassified. JETDS nomenclature is not assigned to software and nonelectrical items.

19. Assignment. COMSEC material is assigned JETDS nomenclature in accordance with the requirements of MIL-STD-196(). Normally, JETDS nomenclature is assigned when sufficient technical information exists to distinguish the item from all other items.

20. Type Designators for COMSEC Material. A type designator for COMSEC hardware consists of the following elements:

a. The nomenclature system designator "AN" followed by a slant (/).

b. A descriptive trigraph followed by a dash. Descriptive trigraphs are taken from ANNEX C and consist of an installation designator to show the type of installation in which the equipment is used, a type indicator to show the general type of equipment, and a purpose designator to show the general purpose of the equipment.

c. A unique item number.

SECTION VII - NOMENCLATURE FOR MISCELLANEOUS COMSEC AIDS

21. Short Titles for NATO COMSEC Aids. Short titles for NATO COMSEC aids are comprised of the following elements, in the order shown:

a. The nomenclature system designator "AMS."

b. The Type Aid Designator.

(1) A. Authentication System

(2) C. Code/Cipher

(3) D. One-Time Pad

(4) G. General Publication

(5) H. Changing Call Sign/Frequency

(6) I. Recognition and Identification

(7) K. Key List

(8) L. Miscellaneous

(9) M. Maintenance Manual

(10) O. Operating Manual

(11) T. Tape

c. A unique item number preceded by one space. Training editions of NATO cryptosystems are identified by the digraph "(TC)" inserted immediately before the item number (e.g., AMSA (TC) 2).

22. Short Titles for Combined Nomenclature. Short titles for COMSEC aids used mutually by Australia, New Zealand, Canada, the United Kingdom, and the United States are comprised of the following elements, in the order shown.

a. The nomenclature system designator "CC."

b. The type aid designator selected from ANNEX B.

c. An item number preceded by one character space.

d. An edition letter or number preceded by one character space.

23. Special Nomenclature.

a. Short titles assigned to COMSEC aids may be tailored to meet department or agency requirements. These short titles may identify the user or communications system (e.g., FBI-1, DCL), or as otherwise requested by the customer.

b. COMSEC aids produced by NSA for internal use by foreign nations bear short titles tailored specifically for the nation involved. The final character of the first part of each short title indicates the type aid and is selected from ANNEX B (e.g., ROKT).

3 Encls:

1. ANNEX A, FUNCTIONAL AND TYPE DESIGNATORS FOR COMSEC EQUIPMENT, EQUIPMENT SYSTEMS, AND ASSEMBLIES

2. ANNEX B, FUNCTIONAL RELATIONSHIP, PURPOSE, AND TYPE DESIGNATORS FOR COMSEC AIDS

3. ANNEX C, JOINT ELECTRONICS TYPE DESIGNATION SYSTEM (JETDS) TABLE OF EQUIPMENT INDICATORS

ANNEX A

FUNCTIONAL AND TYPE DESIGNATORS FOR COMSEC EQUIPMENT, EQUIPMENT SYSTEMS, AND ASSEMBLIES

FUNCTION	TYPE	ASSEMBLY
C - COMSEC Equipment System	G - Key Generation	A - Advancing
K - Cryptographic	I - Data Transmission	B - Base or Cabinet
H - Crypto-Ancillary	L - Literal Conversion	C - Combining
M - Manufacturing	N - Signal Conversion	D - Drawer or Panel
N - Noncryptographic	O - Multipurpose	E - Strip or Chassis
S - Special Purpose	P - Materials Production	F - Frame or Rack
	S - Special Purpose	G - Key Generator
	T - Testing & Checking	H - Keyboard
	U - Television	I - Translator, Reader
	W - Teletypewriter	J - Speech Processing
	X - Facsimile	K - Keyer, Permuting
	Y - Speech	L - Repeater
		M - Memory or Storage
		O - Observation
		P - Power Supply, Converter
		R - Receiver
		S - Synchronizing
		T - Transmitter
		U - Printer
		V - Removable COMSEC Component
		W - Logic Programmer/ Programming
		X - Special Purpose

Element Designators: E, plus an alphabetic trigraph
Element designators include microcircuit boards and printed circuit boards

Subassembly Designators: Z, plus an alphabetic trigraph

Microcircuit Chip Designators: U, plus an alphabetic trigraph

ANNEX B

FUNCTIONAL RELATIONSHIP, PURPOSE, AND TYPE DESIGNATORS FOR COMSEC AIDS

FUNCTIONAL RELATIONSHIP

C - Two-Man Control
E - Electronic EKMS Cryptographic
F - SDNS[1]
G - Type 2
K - Cryptographic
H - Ancillary
M - Manufacturing
N - Noncryptographic
S - Special Purpose
W - Two-Man Control Split Knowledge
Y - Split Knowledge

PURPOSE

A - Operational
B - Compatible Multiple Key
E - Encrypted Operational[2]
L - Logistics Combinations
M - Maintenance
R - Reference
S - Sample
T - Training
V - Developmental
X - Exercise
Z - On-the-Air Test

TYPE AID

A - Authenticator
B - Diagnostic Test Program
C - Code or Cipher System
D - EKMS
E - Floppy Disk
F - Cryptovariable Program
G - General Publication
H - Call Sign or Frequency Changing System
I - Recognition or Identification System
J - Indicator List
K - Key List or Printed Tape
L - Miscellaneous
M - Maintenance Manual
N - Computer Keying
O - Operating Manual
P - One-Time Pad
Q - Engineering Document
S - Sealed Authentication System
T - Punched Tape
U - PROM/ROM/LSI Devices
V - CEOI/JECOI/SOI
W - CRIB
X - Smart Card
Y - Key Card
Z - Permuting Plug

MANUFACTURING AIDS[3]

B - Blue Line
C - Contour Notch Pattern
F - Checking Aid
G - Generation Program
K - Keying Specification
L - Miscellaneous
M - Manuscript
N - Negative
P - Page Proof
R - Repro Page
S - Sample
T - Tape (mag or punched)
W - Wiring Diagram

FORM[4]

A - Punched Card
B - Floppy Disk
D - Magnetic Card
E - Magnetic Tape
F - Microfiche
I - Video Disk
V - Video Cassette

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

1
2
3
4

ANNEX C

JOINT ELECTRONICS TYPE DESIGNATION SYSTEM (JETDS)
TABLE OF EQUIPMENT INDICATORS

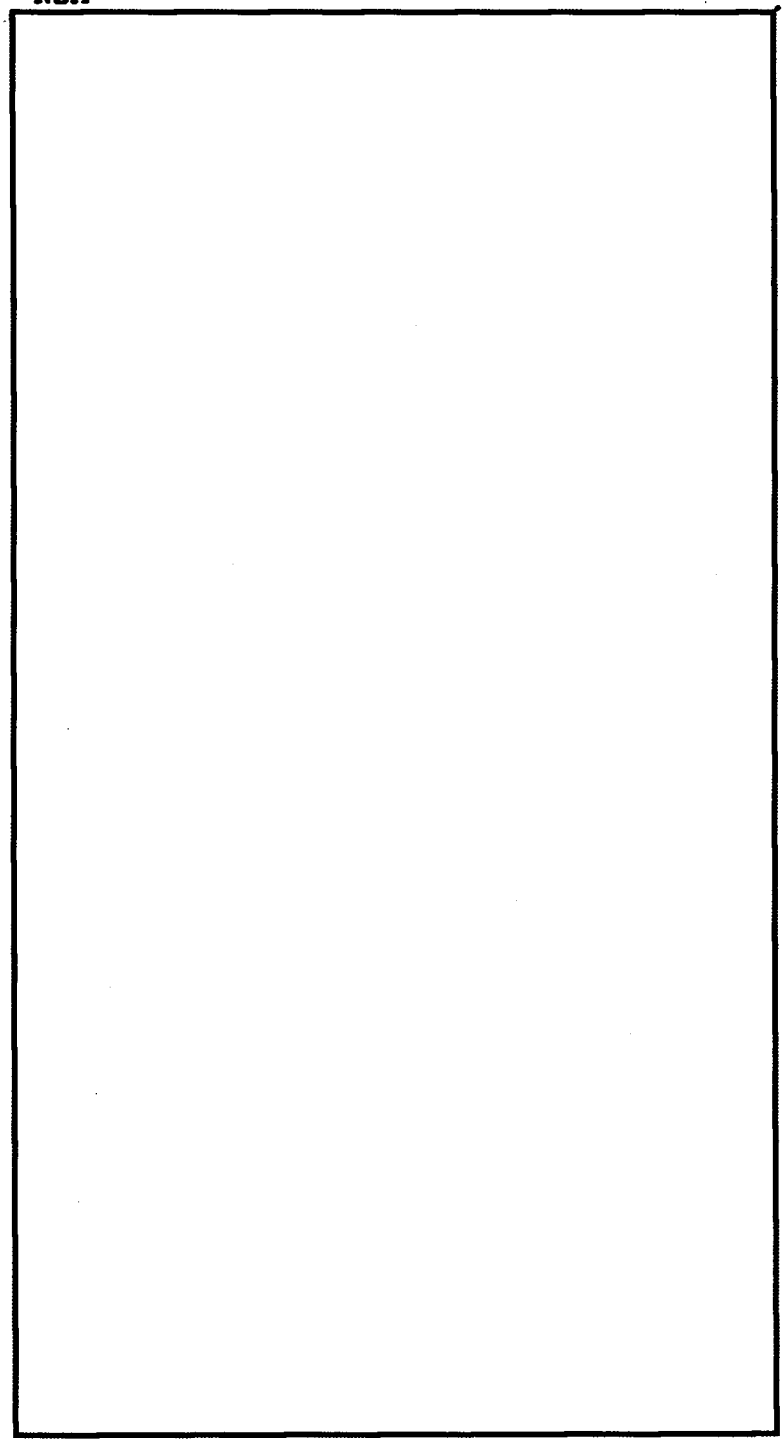
INSTALLATION	TYPE	PURPOSE
A - Piloted Aircraft	A - Invisible Light, Heat Radiation	B - Bombing
B - Underwater Mobile, Submarine	C - Carrier	C - Communications
C * Cryptographic	D - Radiac	D - Direction Finder, Reconnaissance and/or Surveillance
D - Pilotless Carrier	G - Telegraph or Teletype	E - Ejection and/or Release
F - Fixed Ground	I - Interphone and Public Access	G - Fire Control or Searchlight Directing
G - General Ground Use	J - Electromechanical or Inertial Wire Covered	H - Recording and/or Reproducing
K - Amphibious	K - Telemetering	K - Computing
M - Mobile (Ground)	L - Countermeasures	M - Maintenance and/or Test Assemblies
P - Portable	M - Meteorological	N - Navigational Aids
S - Water	N - Sound in Air	Q - Special or Combination
T - Transportable	P - Radar	R - Receiving and/or Passive Detection
U - General Utility	Q - Sonar and Underwater Sound	S - Detecting and/or Range and Bearing, Search
V - Vehicular	R - Radio	T - Transmitting
W - Water Surface and Underwater Combined	S - Special or Combined	W - Automatic Flight or Remote Control
Z - Piloted-Pilotless Airborne Vehicles Combined	T - Telephone (Wire)	X - Identification and Recognition
	V - Visual and Visible Light	Y - Surveillance and Control combined
	W - Armament	Z * Secure
	X - Facsimile or Television	
	Y - Data Processing	
	Z * Communications	

* [redacted] (b)(3)-18 USC 798 (b)(3)-P.L. 86-36

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

AS OF: 7 OCTOBER 1993

DISTRIBUTION:
NSA



~~FOR OFFICIAL USE ONLY~~

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