

EXECUTIVE SECRETARIAT**ROUTING SLIP**

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS		X (for SECOM)		
5	DDI				
6	DDA		X (for D/OC)		
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI		NS/DHS		
18	C/IPD/OIS				
19	NIO				
20					
21					
22					

SUSPENSE _____
Date

Remarks

STAT

Amj for Executive Secretary
 30 Jan 85
 Date

3637 (10-81)

~~FOR OFFICIAL USE ONLY~~

1-3/5

NTISSC

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY
COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

NTISSC 1-3/58#85
NTISSC 1-3/58
28 January 1985

MEMORANDUM FOR THE MEMBERS AND OBSERVERS,
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY
COMMITTEE (NTISSC)

SUBJECT: Telecommunications Protection Bulletin

The enclosed copy of the "Telecommunications Protection
Bulletin" is forwarded for your information. Upon request,
additional copies of this publication may be obtained from:

31 JAN 1985

Comm

[Redacted]
National Security Agency
Operations Building #3, Room C2A19
Fort George G. Meade, Md. 20755-6000
Phone: 699-7110.

[Signature]
[Redacted]
Executive Secretary

1 Encl:
a/s

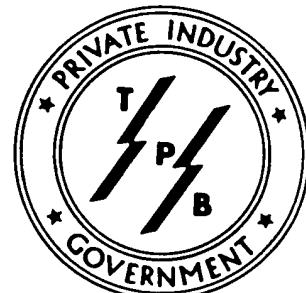
DCI
EXEC
REG

~~FOR OFFICIAL USE ONLY~~

TELECOMMUNICATIONS

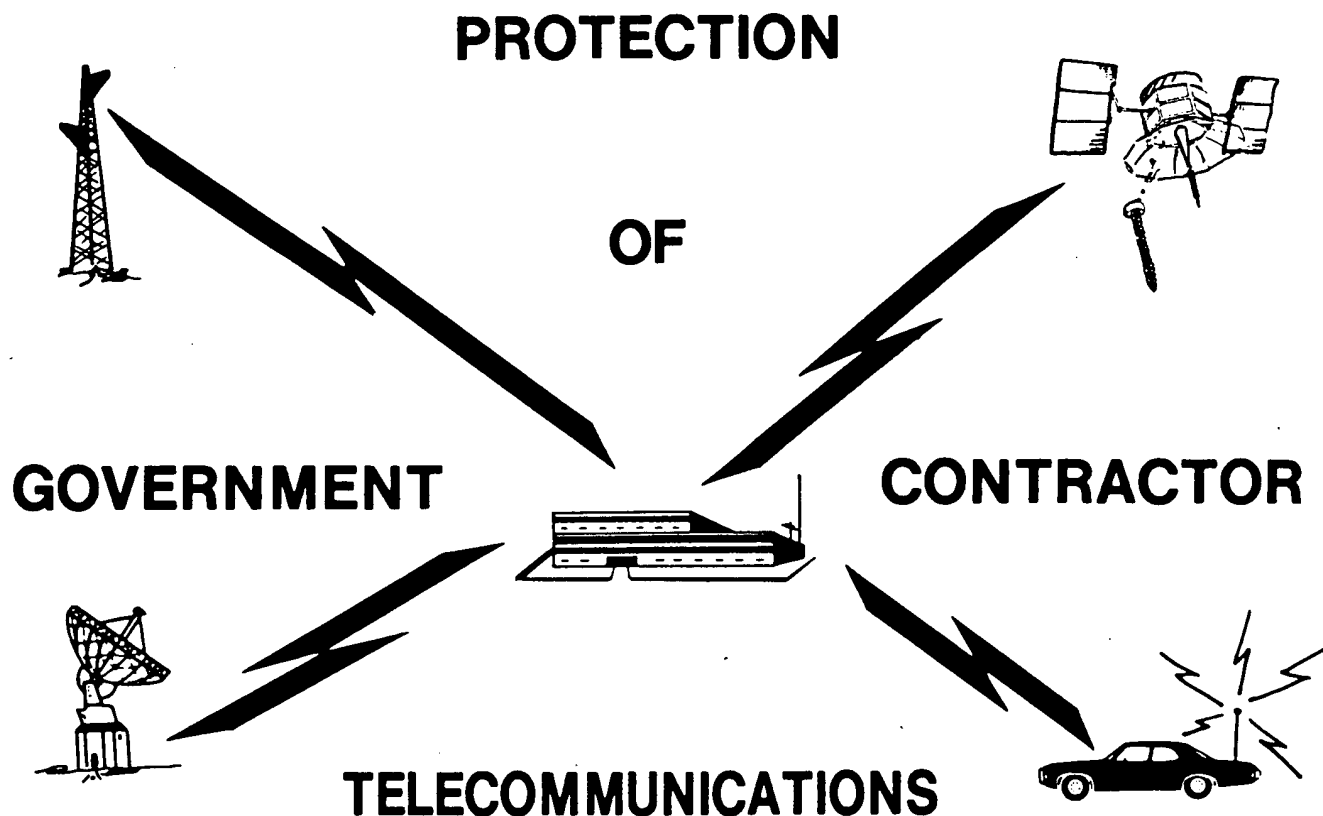


PROTECTION BULLETIN



VOLUME I. NO. 2

NOVEMBER 1984



THE TELECOMMUNICATIONS PROTECTION BULLETIN IS ISSUED APERIODICALLY BY THE NATIONAL SECURITY AGENCY TO THOSE GOVERNMENT CONTRACTORS WHO HAVE A NEED TO BE KEPT INFORMED ON MATTERS RELATING TO THE IMPLEMENTATION OF NATIONAL POLICIES FOR THE PROTECTION OF GOVERNMENT CONTRACTOR TELECOMMUNICATIONS. IT IS NON-DIRECTIVE IN NATURE, IS ISSUED FOR INFORMATION PURPOSES ONLY, AND SHOULD NOT BE CITED AS AUTHORITY FOR OFFICIAL ACTIONS. THE INFORMATION CONTAINED IN THE BULLETIN IS PROVIDED FOR OFFICIAL USE WITHIN GOVERNMENT CONTRACTOR FACILITIES AND IS NOT RELEASABLE TO THE GENERAL PUBLIC. IT MAY BE REPRODUCED, ALL OR PART, FOR THIS PURPOSE.

FOR OFFICIAL USE ONLY



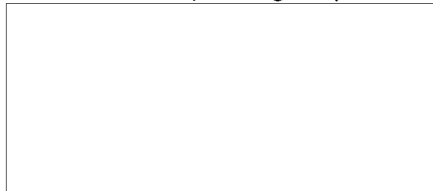
NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

FOREWORD

In the last edition of the TPB, I alerted you to the threat to our national security posed by the exploitation of our nation's unprotected communications. This threat is growing in both intensity and diversity. Because our adversaries find themselves incapable of supplying their own technological progress, or find it more economical, they steal it from us by the most efficient means available; exploitation of the unprotected communications of American industry.

The rapid advancement of state-of-the-art communications technology in today's "Information Age" dictates that prompt and profound changes are necessary to the ways that we have, in the past, developed and implemented the means to protect our telecommunications. To meet this challenge and make the changes required by this new era of telecommunications protection, we have developed a plan that we call the "New Way of Doing Business." Essentially, it is a plan that requires a close working relationship between the private sector and government to harness our country's technology advantages and free market economy in an efficient and competitive manner to meet our vast communications protection needs.

More detailed information about our "New Way of Doing Business" will be forthcoming in future editions of the TPB. Advance information about the Commercial COMSEC Endorsement Program (CCEP), one of the new initiatives already being implemented under this plan, is included in this edition.



Deputy Director
for
Communications Security

i
FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

<u>PAGE</u>	<u>SUBJECT</u>
i	FOREWORD
ii	TABLE OF CONTENTS
1	GENERAL
1	SECRETARY OF DEFENSE DIRECTS NEW PROCEDURES
2	COMMERCIAL COMSEC ENDORSEMENT PROGRAM (CCEP)
3	NEW SECURE TELEPHONE SYSTEM
4	COMMON CARRIER PROTECTED COMMUNICATIONS SERVICE
5	APPROVED SATELLITE PROTECTION
5	AVAILABILITY OF KEY FILL DEVICE KOI-18
5	MARKET OF TSEC/KY-71A AND TSEC/KG-84A TO GOVERNMENT CONTRACTORS
6	TELECOMMUNICATIONS PROTECTION AWARENESS
7	NSA ASSISTANCE
7	COMPANY PROPRIETARY INFORMATION
8	TPB DISTRIBUTION
9	TPB DISTRIBUTION ACTION REQUEST FORM
APPENDIX I - LIST OF PREVIOUSLY PUBLISHED TPB'S	
APPENDIX II - LIST OF PROTECTION EQUIPMENT AND VENDOR CONTACTS	
APPENDIX III - NACSI 6002 (PROTECTION OF GOVERNMENT CONTRACTOR TELECOMMUNICATIONS)	

GENERAL

Each new edition of the TPB is published primarily to keep you informed about the latest developments on matters related to the protection of Government contractor telecommunications. Therefore, most of the information contained in each succeeding edition of the TPB is not cumulative.

Appendix I to this TPB contains a list of all previously published editions of the TPB and the significant subjects addressed in each. Previously published editions of the TPB, less the List of Protection Equipment and Vendor Contacts which is cumulative in each new edition, will be provided to you upon request. You must use the TPB Distribution Action Request Form (page 9) for this purpose.

SECRETARY OF DEFENSE DIRECTS NEW PROCEDURES TO ENHANCE PROTECTION OF GOVERNMENT CONTRACTOR TELECOMMUNICATIONS

On 9 October 1984 the Secretary of Defense (SECDEF), in a memorandum to key DoD officials, directed the establishment of new procedures designed to enhance and accelerate the protection of Government contractor telecommunications. Issued on the heels of National COMSEC Instruction (NACSI) No. 6002 (attached as Appendix III to this TPB), the Secretary's memorandum outlined how, under previous procedures, contractors had to rely on Government Furnished Equipment (GFE) in order to secure their classified telecommunications. Secretary Weinberger then announced that NSA had established a new procedure whereby Defense contractors would be able to purchase COMSEC equipment or services direct from government authorized vendors. The cost of "securing" the transmission of classified information and "protecting" the transmission of unclassified sensitive information is to be charged to the government, similar to the way other security costs are charged. This program will relieve the burden on the government for GFE and will enable contractors to rapidly obtain appropriate security or protection for their telecommunications. The SECDEF memorandum is quoted, in part, for your information:

"QUOTE":

9 October 1984

MEMORANDUM FOR THE SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL
INSPECTOR GENERAL
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Protection of Government Contractor Telecommunications

Our adversaries' attention to national security or national security-related information transmitted between and among the Government and its Defense contractors is well documented, and the threat to our national interests is all too clear.

FOR OFFICIAL USE ONLY

In the past, DoD provided limited quantities of COMSEC material to contractors as Government Furnished Equipment (GFE) and encouraged them to procure protection equipment for other needs, at their own expense. NSA has established alternative procedures which authorize defense contractors to satisfy security by direct purchase of COMSEC material or services from Government-authorized commercial vendors. This new arrangement, when coupled with existing provisions of the Federal Acquisition Regulations, will allow you to require in future contracts and amendments that Defense contractors procure their own COMSEC or protected equipment or services and recover acquisition, operations, maintenance and related administrative costs in the same manner as they now do for other security requirements imposed by or allowed in contracts. This new procedure will also relieve a significant burden on the Government COMSEC program by establishing suppliers with inventories of COMSEC assets and should eliminate the need for emergency loans from the military COMSEC pipeline.

I believe it vital that we move aggressively to exploit this innovative, cooperative government-industry program....

For purposes of this program, the term "Unclassified, National Security-Related (UNSR) Information" is defined as information related to a DoD contractor (including pre-award) that involves programs, materials, products, or technologies that are controlled by the Department of Defense under appropriate statutory authority, for example, 10 U.S.C. 140c.

The Director, National Security Agency, will publish quarterly an approved Communications Security and DES equipment and vendors' list.

All Departments and Agencies are to develop procedures for execution of this initiative and to provide a status report to the Deputy Under Secretary of Defense (Policy) on implementation progress.

(SIGNED)
Caspar W. Weinberger

"UNQUOTE"

COMMERCIAL COMSEC ENDORSEMENT PROGRAM (CCEP)

NSA is establishing a Commercial COMSEC Endorsement Program (CCEP) in an attempt to involve qualified companies within the private sector in our efforts to develop and implement new cryptographic devices for Government and Government contractor use. The program is intended to produce specifications and procedures for standard cryptographic designs and techniques that can be provided to industry to allow development and production of a wide variety of NSA-approved secure telecommunications systems. This program is intended to use competition to encourage the timely and economical development of secure communications systems, not just security add-ons as an afterthought. The goal is to ensure commercially developed telecommunications systems that are sold to the Government market will meet appropriate security standards for transmission of classified information. Endorsement of a telecommunications product by NSA assures authorized users that the system adheres to a specified level of security integrity.

Although the program is in the early stages of development, several telecommunications vendors have shown interest and a few have already entered into formal agreements to participate. These companies develop and sell a variety of voice and data telecommunications products. Secure telecommunications systems developed through this program should be available starting in 1986.

Inquiries regarding the CCEP should be directed to Mr. Dennis Grayson:

Mail: Director
National Security Agency
ATTN: S94
Fort George G. Meade, MD 20755-6000

Telephone: 301-688-7110

NEW SECURE TELEPHONE SYSTEM

In response to the increasing need to protect sensitive telephone conversations from unauthorized intercept, the National Security Agency has begun a joint initiative with the telecommunications industry to develop and field a new secure telephone system for widespread use throughout the U.S. The primary goal is to provide a family of low cost, user friendly secure telephone units, with excellent voice quality, meeting a broad variety of needs. The telephone units will be available in versions compatible with conventional office requirements and standard telephone systems/PBX's, as well as cellular mobile radio-telephone systems, and portable/briefcase applications. U.S. Government contractors will be able to purchase appropriate members of the secure telephone family directly from the manufacturer.

The major features of the Secure Telephone System include:

- Unit Price Goal - \$2,000.
- Equipment unclassified when unkeyed.
- Easy to install and simple to operate.
- Size of a conventional multi-line deskset.
- Multilevel Security with positive authentication of the far-end terminal's authorized classification level.
- High Quality, full duplex communication over a single telephone line.
- Direct support from the manufacturer for installation, keying, and maintenance.
- Optional secure data capabilities.
- Secure telephone units available for direct purchase from a minimum of two vendors.

Within the Secure Telephone Family members, there will be two generic terminal types. The Type I terminal will provide adequate security to protect all levels of classified communications. These will be available to U.S. Government Agencies and Departments, as well as Government contractors holding classified contracts. The Type II Terminal will be designed for the protection of unclassified communications, will be interoperable with the Type I, and will be available to the U.S. Government and the general U.S. private sector. A visual display on the terminal will provide a positive authentication of the far-end terminal's location/user and authorized classification level. For example, on a call to the National Security Agency, the display on the calling parties' terminal would read:

FOR OFFICIAL USE ONLY

TOP SECRET

NATIONAL SECURITY AGENCY

FORT GEORGE G. MEADE, MD

The Secure Telephone Units are expected to be available in 1987. This secure telephone system will provide a viable means for Government agencies and contractors to satisfy their NACSI 6002 requirements to protect sensitive voice communications. For further information please call Linda Pellicani or Stan Hedy at the National Security Agency on (301) 688-7897.

COMMON CARRIER PROTECTED COMMUNICATIONS SERVICE

Arrangements have been made with the major long-haul commercial common carriers to provide NSA-approved protection for the transmission of unclassified national security-related (UNS-R) information. Protected service includes routing traffic over wire cable, fiber optics, or bulk-protected microwave. It can be provided in specific geographic areas defined by NSA as being the highest priority for protection. Further details concerning the various approved protection options that are available may be obtained from the following point of contact at the common carrier company indicated:

1. ITT/UNITED STATES TRANSMISSION SYSTEM (USTS)

Mr. Frank D'Agostino
1600 M Street, N.W.
Washington, DC 20036

Tel: 202-775-7318

2. WESTERN UNION TELEGRAPH COMPANY

Mr. Dave Stem
Government Electronics Division
7916 Westpark Drive
McLean, VA 22102

Tel: 703-790-2347

3. GTE/SPRINT

Mr. Jay Nelson
1828 L Street N.W.
Suite 500
Washington, DC 20036

Tel: 202-822-0002

4. MCI TELECOMMUNICATIONS

Mr. Jerry L. Gibson
601 S. 12th Street
Arlington, VA 22202

Tel: 703-486-4360

FOR OFFICIAL USE ONLY

5. AT&T COMMUNICATIONS

Mr. Richard Hermit
1120 20th Street N.W.
Washington, DC 20036

Tel: 202-457-2907

APPROVED SATELLITE PROTECTION

NSA has approved a 48 Megabit Satellite Bulk-Encrypted Transmissiton Service offered by Satellite Business Systems for protecting unclassified national security-related information. Inquiries about this protected service may be directed to:

Mail: Mr. Larry A Weekley
Satellite Business Systems
8283 Greensboro Drive
McLean, VA 22102

Telephone: 703-442-5577

AVAILABILITY OF KEY FILL DEVICE KOI-18

The KOI-18 may be used with many of the NSA-approved commercial protection devices. Manufacturers of the protection devices offer a special cable for this purpose. In the past, KOI-18's have been available to Government contractors only as Government Furnished Equipment (GFE) at the largess of a Government contract sponsor. In the very near future, Government contractors may purchase KOI-18's direct from the manufacturer for use with approved protection devices. Inquires concerning the purchase of KOI-18's may be directed to:

Mail: Mr. Edward D. Elmo
Systems Development Corp./A Burroughs Co.
P.O. Box 517
Paoli, PA 19301

Telephone: 215-363-4627

MARKET OF TSEC/KY-71A AND TSEC/KG-84 TO GOVERNMENT CONTRACTORS

In order to facilitate compliance with NACSI 6002, NSA has authorized the manufacturers of the TSEC/KY-71A and the TSEC/KG-84A to market these equipments directly to government contractors. The manufacturers are also authorized to offer a wide range of services associated with the applications of these equipments including training, installation, and maintenance. NSA will provide the crypto keying material. Inquiries about prices and availability of the TSEC/KY-71A and the TSEC/KG-84A should be directed to the following manufacturer point-of-contact (POC) for the equipment indicated.

TSEC/KY-71A Secure Telephone Unit (STU-II)

Manufacturer (1): The ITT Corporation

POC: Mr. John Dalton

FOR OFFICIAL USE ONLY

Mail: The Defense Communications Division
492 River Road
Nutley, NJ 07110

Telephone: 201-284-3168

TSEC/KG-84A General Purpose Encryption Equipment

Manufacturers (2):

(1) Bendix Corporation

POC: Mr. Lou Hause

Mail: Bendix Corporation
1300 East Joppa Road
Baltimore, MD 21204

Telephone: 301-583-4486

(2) TRW/EPI

POC: Mr. Dale Johnson

Mail: TRW/EPI
3450 N. Nevada Avenue
Colorado Springs, CO 80907

Telephone: 303-475-0660

TELECOMMUNICATIONS PROTECTION AWARENESS

This item will appear in every edition of the TPB. It will contain information about ideas and techniques that you may use as part of your company's telecommunications protection awareness programs, or be used to inform you of any specific problem areas that have come to our attention. This edition features:

"The Unprotected Telephone"

Your office or home telephone is your link with the outside world in every sense. The more you use your telephone, especially for long distance calls, the more accessible you are to undetected eavesdropping by foreign agents--or terrorists, criminals, or industrial spies.

Telephone monitoring is relatively easy. Most domestic long distance calls are transmitted over terrestrial microwave radio relays or satellite. Although these terrestrial microwave relays are intended as point-to-point transmissions, the transmitted signal, in fact, carries many miles beyond the intended receiving tower. In addition, each transmitting microwave relay tower radiates its signal to both sides and to the rear. Your conversation, in effect, is broadcast over a wide area.

Communications satellites, which are used as space-based communications repeater stations between earth terminals, are similarly subject to intercept. Though they operate on different frequencies than microwave systems, the two are easily interconnected. Thus, telephone calls placed from home or businesses may travel via cable, microwave, or a combination of the two and be repeated along a satellite path. The radio signals up to and down from the satellite are, like microwave transmissions, vulnerable to intercept, although the equipment need is considerably more sophisticated than that required for terrestrial microwave interceptions. Furthermore, most domestic satellite transmissions can be intercepted from appropriate locations outside the borders of the United States.

The intercept and analysis of microwave transmissions have been facilitated significantly by advancement in antenna design and electronic components, and by the development of high-speed, large volume computers. No physical connection is necessary to intercept microwave transmissions, only possession of the proper receiver and the ability to place an antenna within range of the radiated microwave signal. Detection of such intercept efforts is extremely difficult. Thus, a properly equipped interceptor can, with a minimum risk of exposure, easily collect information from almost any user of our telephone system.

NSA ASSISTANCE

We are committed to working with you in your efforts to protect your telecommunications. Your principal point of contact for the protection of Government contractor communications is:

Name

William (Bill) F. Winters

Telephone Number

(301) 688-7110/8124

Address

Director
National Security Agency
ATTN: S99
Fort George G. Meade, MD 20755

COMPANY PROPRIETARY INFORMATION

"The National Security Agency will hold in strict confidence and limit the internal dissemination of all information and data provided by a company with whom the Agency is working with to protect their company telecommunications. The company should clearly identify all trade secrets and commercial or financial data provided to the Agency on a privileged or confidential basis so that such business information can be protected to the full extent authorized by the Freedom of Information Act (FOIA). If required, NSA will actively solicit an effected company's assistance in establishing supportable bases for protecting company information and data in response to any FOIA requests."

FOR OFFICIAL USE ONLY

TPB DISTRIBUTION

Since telecommunications protection is inherently both a security and telecommunications issue which generally requires a concerted effort by the two elements, we recommend that both these company elements receive the TPB. Subject to our approval, we will send it to whomever you wish, to include all your various company locations, subsidiaries, etc.

The accurateness of our mail address list used to distribute the TPB is based upon information supplied to us by you, the TPB recipients. You should keep us informed of any additions, deletions, or changes required. The form on page 9 is furnished for this purpose.

17. P. E. Systems TED 417/1027

The P. E. Systems TED 417/1027 is an asynchronous digital data which can operate up to 9600 BPS.

Keying variables are entered into the TED 417/1027 via a KOI-18. To enter keying variables via a KOI-18, you require special cables and a punched DES key tape. Cables can be ordered from P. E. Systems.

Cost for the P. E. System TED 417/1027 is expected to be in the \$2,500.00 range.

The P. E. Systems TED 417/1027 is identified as USGEID 00000017.

¹ Every DES equipment that NSA endorses is identified by the term "USGEID" and an eight digit code. This equipment designator shall be permanently affixed to the equipment by the manufacturer and be readily visible to the purchaser at the time of purchase.

LIST OF PREVIOUSLY PUBLISHED TPBs

VOLUME I, NO. 1, JANUARY 1984

Significant Subjects:

(1) FOREWORD: The NSA Deputy Director for Communications Security advised about the serious threat to our national security posed by the drain of UNS-R information to our adversaries through exploitation of the nations unprotected telecommunications.

(2) UNS-R INFORMATION: Offered a definition of the term "Unclassified National Security-Related (UNS-R)" and some examples of this type information.

(3) APPROVED PROTECTION: Explanation of "approved" protection under the provisions of NCSC-11 as it relates to "endorsed" DES equipments.

(4) NSA-ENDORSED DES EQUIPMENTS: Explanation of the NSA DES Endorsement Program.

(5) NATIONAL POLICIES: Advised that NCSC-10 (National Policy for Protection of U.S. National Security-Related Information Transmitted Over Satellite Circuits) and NCSC-11 (National Policy for Protection of Telecommunications Systems Handling Unclassified National Security-Related Information) had been widely distributed to Government contractors and that those who did not have them could get them by submitting a request to us.

Appendix I to TPB Volume 1, No. 2, November 1984

FOR OFFICIAL USE ONLY

LIST OF PROTECTION EQUIPMENT & VENDOR CONTACTS

1. NSA Endorsed Equipments: Prior NSA approval is not required for the application of these equipments to protect UNS-R information. The enclosure to this Appendix contains detailed information about each type of equipment listed. The page number where each type of equipment can be found in the enclosure is provided for your convenience.

Motorola Voice Radio Equipment Pages 1,2,3,4,5,6

Phil Lerner, Camp Springs, MD
Tel: 301-899-3950

Low Speed Data Equipments

(1) Paradyne Page 8

Frank Dolan, McLean, VA
Tel: 703-448-0062

(2) Racal-Milgo Page 8

Wayne Braunstein, Wash DC
Tel: 202-466-3940

(3) P.E. Systems Page 9

Jeanne Wilgus, Alexandria, VA
Tel: 703-642-9300

High Speed Data Equipments

(1) California Microwave Page 6

Dennis King, Sunnyvale, CA
Tel: 408-720-6467

(2) M/A-COM Linkabit Page 7

Ken Cohen, San Diego, CA
Tel: 619-457-2340

2. Equipments Under Evaluation for Endorsement: Applications of these equipments must be approved by NSA on a case-by-case basis until the evaluation process is completed.

Low Speed Data Equipments

Analytics: Jim Passmore, McLean, VA
Tel: 703-471-0892

Appendix II to TPB Volume I, No. 2, November 1984

FOR OFFICIAL USE ONLY

Local Area Network

SYTEK: Bill Taylor, Rockville, MD
Tel: 301-530-5100

Telephone and Radio

DATOTEK: Sue Robinson, Dallas, TX
Tel: 214-241-4491

Teletype

Teletype Corp: John Daleiden, Skokie, IL
Tel: 312-982-2519

3. Keying Material: NSA will provide the cryptographic keying material, free of charge, for the protection of UNS-R information.

23 October 1984

DES Equipment
Endorsed by NSA as Meeting Federal Standard I027

1. Motorola DES Key Variable Loader T3020-X.
The DES key variable loader costs \$1,821.
The DES key variable loader is identified as USGEID 00000001¹.
2. Motorola DES Handheld Radios (MX-300 series with individual channel elements).

H23AXU1120_N	H33AXU1120_N	H43AXU1120_N	On 1 Jan 84,
H23AXU1140_N	H33AXU1140_N	H43AXU1140_N	Motorola dis-
H23AXU1160_N	H33AXU1160_N		continued
H23AXU3120_N	H33AXU3120_N	H43AXU3120_N	manufacturing
H23AXU3140_N	H33AXU3140_N	H43AXU3140_N	these radios
H23AXU3150_N	H33AXU3160_N		

H24AXU1120_N	H34AXU1120_N	H44AXU1120_N
H24AXU1140_N	H34AXU1140_N	H44AXU1140_N
H24AXU1160_N	H34AXU1160_N	H44AXU1160_N
H24AXU1180_N	H34AXU1180_N	H44AXU1180_N
H24AXU3120_N	H34AXU3120_N	H44AXU3120_N
H24AXU3140_N	H34AXU3140_N	H44AXU3140_N
H24AXU3160_N	H34AXU3160_N	H44AXU3160_N
H24AXU3180_N	H34AXU3180_N	H44AXU3180_N

The handheld radios must be purchased with the H388 DES Option. The H388 DES coding algorithm module, which replaces the Motorola proprietary DVP algorithm, costs \$106.

The Motorola handheld radios range in cost from \$3,120 for the H23AXU1120_N to \$4,444 for the H44AXU3180_N.

The Motorola MX-300 DES Handheld Radios are Identified as USGEID 00000002.

3. Motorola DES Mobile Radios

T43TXA1200_K	T83TXA1200_K	
T43TXA1D00_K	T83TXA1D00_K	
T43TXA1J00_K	T83TXA1J00_K	
T43TXA3200_K	T83TXA3200_K	
T43TXA3D00_K	T83TXA3D00_K	
T43TXA3J00_K	T83TXA3J00_K	
T34TXA1200_K	T44TXA1200_K	T74TXA1200_K
T34TXA1D00_K	T44TXA1D00_K	T74TXA1D00_K
T34TXA1J00_K	T44TXA1J00_K	T74TXA1J00_K
T34TXA3200_K	T44TXA3200_K	T74TXA3200_K
T34TXA3D00_K	T44TXA3D00_K	T74TXA3D00_K
T34TXA3J00_K	T44TXA3J00_K	T74TXA3J00_K

Enclosure to Appendix II to TPB Volume 1, No. 2, November 1984

1

FOR OFFICIAL USE ONLY

Motorola DES Mobile Radios must be purchased with the W388 DES Option and the W391 Security Option. The W388 DES coding algorithm module, which replaces the Motorola proprietary DVP algorithm, costs \$106. The W391 Security Option, which protects the DES and related electronics in a lockable security enclosure costs \$283.

The Motorola Mobile Radios range in cost from \$3,090 for the T43TXA1200_K to \$4,022 for the T74TXA3J00_K.

The Motorola DES Mobile Radios are identified as USGEID 00000003.

4. Motorola DES Base Stations/Fixed Repeaters

C53RXB1106_T	C73RXB1106_T	C53RXB3106_T	C73RXB3106_T
C53RXB1126	C73RXB1126	C53RXB3126	C73RXB3126
C53RXB1196	C73RXB1196	C53RXB3196	C73RXB3196

C34RXB1106_T	C64RXB1106_T	C34RXB3106_T	C64RXB3106_T
C34RXB1126	C64RXB1126	C34RXB3126	C64RXB3126
C34RXB1196	C64RXB1196	C34RXB3196	C64RXB3196

B84RXB1106_SP
B84RXB1106_TSP
B84RXB3106_SP
B84RXB3106_TSP

B93RXB1106_TSP B93RXB3106_TSP
B93RXB1126SP B93RXB3126SP
B93RXB1196SP B93RXB3196SP

The Motorola DES Base Stations must be purchased with the C388 DES Option, the C557 Security Option, and the TLN2477 Cabinet Security Kit, the TLN2478 Cabinet Security Kit or the TRN5669 Cabinet Security Kit.

The C388 DES coding algorithm module, which replaces the Motorola proprietary DVP algorithm, costs \$106. The C557 Security Option costs \$85. The TLN2477 Cabinet Security Kit costs \$255. The LN2478 Cabinet Security Kit costs \$110.

The Motorola DES Base Stations/Fixed Repeaters range in cost from \$6,758 for the C53RXB1106_T to \$8,415 for the C64RXB3196_T.

The Motorola DES Base Station/Fixed Repeater is identified as USGEID 00000004.

5. Motorola Synthesized DES Handheld Radios (MX-300-S, MX-300-R, PX-300-S)

MX-300-S

H23SXU1140_N	H24SXU1140_N
H23SXU3140_N	H24SXU3140_N

H33SXU1140_N	H34SXU1140_N
H33SXU3140_N	H34SXU3140_N

H43SXU1140_N	H44SXU1140_N
H43SXU3140_N	H44SXU3140_N

MX-300-R

H23SXUII44A	H24SXUII44A
H23SXUII44AN	H24SXUII44AN
H23SXU3I44A	H24SXU3I44A
H23SXU3I44AN	H24SXU3I44AN

H33SXUII44A	H34SXUII44A
H33SXUII44AN	H34SXUII44AN
H33SXU3I44A	H34SXU3I44A
H33SXU3I44AN	H34SXU3I44AN

H43SXUII44A	H44SXUII44A
H43SXUII44AN	H44SXUII44AN
H43SXU3I44A	H44SXU3I44A
H43SXU3I44AN	H44SXU3I44AN

PX-300-S

P1334_X	P1336_X
P1335_X	P1337_X
P1338_X	P1340_X
P1339_X	P1341_X

P1346_X	P1348_X
P1347_X	P1349_X
P1351_X	P1353_X
P1352_X	P1354_X

The Motorola Synthesized Handheld radios must be purchased with the H388 DES Option. The H388 DES coding algorithm, which replaces the Motorola proprietary DVP algorithm, costs \$106.

The Motorola Synthesized Handheld radios range in cost from \$3,430 for the H23SXU1140_N to \$3,996 for the H44SXU3140_N.

The MX-300-R is the exact same radio as the MX-300-S except that it has a housing that meets Mil-Spec-810C. The cost of this Mil-Spec-810C housing is \$180.

The PX-300-S ranges in cost from \$3,764 for the P1334_X to \$4,187 for the P1354_X.

FOR OFFICIAL USE ONLY

The Motorola MX-300-S and the MX-300-R and the PX-300-S are identified as USGEID 00000005.

6. Motorola DES Syntor-X Mobile Radio

T83VXJ7204_K T53VXJ7204_K
T83VXJ7D04_K T53VXJ7D04_K
T83VXJ7J04_K T53VXJ7J04_K

Motorola DES Syntor-X Mobile Radios must be purchased with the W388 DES Option and the W391 Security Option. The W388 DES coding algorithm module, which replaces the Motorola proprietary DVP algorithm, costs \$106. The W391 Security Option, which protects the DES and related electronics in a lockable security enclosure, costs \$283.

The Motorola Syntor-X Mobile Radios range in cost from \$3,935 for the T83VXJ7204_K to \$4,038 for the T83VXJ7J04_K.

The Motorola DES Syntor-X Mobile Radios are assigned USGEID 00000006.

7. Motorola MX-300 DES "Midband" Handheld Radio

H32AXU1120_NSP H42AXU1120_NSP
H32AXU1140_NSP H42AXU3120_NSP
H32AXU3120_NSP
H32AXU3140_NSP

The Motorola MX-300 DES "Midband" Handheld Radio must be purchased with the H388 DES Option. The H388 DES coding algorithm module, which replaces the Motorola proprietary DVP algorithm, costs \$106.

The Motorola MX-300 DES "Midband" Handheld radios are Identified as USGEID 00000007.

8. Motorola DES Coded/Clear Portable Repeater

P43SXS1180_T
P43SXS3180_T
P44SXS1180_T
P44SXS3180_T
P42SXS1180_TSP
P42SXS3180_TSP

The Motorola DES Coded/Clear Portable Repeater must be purchased with the H388 DES Option which costs \$106 and the PLN-6809A Security Option. The Portable Repeater ranges in cost from \$10,943 to \$11,312.

Motorola also builds a "clear/transparent" portable repeater which cannot be modified for DES operation. These equipments are identified as P43SYS1180 T, P43SYS3180 T, P44SYS1180 T and the P44SYS3180 T. These "clear/transparent" Portable Repeaters do not require FS-1027, NSA Endorsement.

The Motorola DES Coded/Clear Portable Repeater is Identified as USGEID 00000008.

9. Motorola DES Console Interface Unit (CIU)

Q2209CA	Q2209CE	Q2209CJ
Q2209CB	Q2209CF	Q2209CK
Q2209CC	Q2209CG	Q2209CL
Q2209CD	Q2209CH	Q2209CM

The Motorola CIU must be purchased with the C388AA DES option, the C557AA or the C557AB Security-Anti Tamper option, and either the TLN2477A, the TLN2478A, the TRN5669A, or the TRN5670A Cabinet Security Kit option depending upon the cabinet size or configuration.

The C388AA DES coding algorithm module, which replaces the Motorola proprietary DVP algorithm, costs \$106. The C557AA or the C557AB Security-Anti Tamper option costs \$85. The TLN2477A Cabinet Security Kit costs \$255, the TLN2478A Cabinet Security Kit costs \$110, the TRN5669A Cabinet Security Kit costs \$100 and the TRN5670A costs \$100.

The Motorola CIU's range in cost from \$2,475 for the Q2209CA to \$3,801 for the Q2209CM.

The Motorola DES Console Interface Unit is identified as USGEID 00000009.

10. Motorola Spectra-TAC Comparator

Q2208BA

The Motorola DES Spectra-TAC Comparator must be purchased with the C388ABSP DES option, the C557ACSP Security-Anti Tamper and either the TLN2477A, the TLN2478A, the TRN5669A or the TRN5670A Cabinet Security Kit option depending upon the cabinet size or configuration.

The C388ABSP DES option, which replaces the Motorola proprietary DVP algorithm, costs \$106. The C557ACSP Security-Anti Tamper option costs \$85. The TLN2477A Cabinet Security Kit costs \$255, the TLN2478A Cabinet Security Kit costs \$110, the TRN5669A costs \$100 and the TRN5670A costs \$100.

The Motorola Q2208BA DES TAC Comparator costs \$3,925.

The Motorola DES TAC Comparator is identified as USGEID 00000010.

11. CALIFORNIA MICROWAVE VIDAR 5800

The California Microwave Vidar 5800, which meets FS-1027, is a bulk encryption device which operates at speeds of 1.544 megabits in a DS-1 format with a power requirement of 85 watts -24 to -48Vdc.

The California Microwave Vidar 5800 requires a KOI-18 with special cables to load the DES key. The DES key must be ordered in a punched paper tape format. Questions concerning the special cables for the KOI-18 should be directed to California Microwave Bill Lattin 408-732-4000, ext. 225.

NSA has not approved as meeting FS-1027 any of the Vidar 5800 accessories (e.g. 5845 Electronic Keyloader, 5590 110 Vac Power Supply, etc.)

Cost for the California Microwave Vidar 5800 is expected to be in the \$10,000 range.

The California Microwave Vidar 5800 is identified as USGEID 00000011.

12. Motorola DES MCX-100 Mobile Radio

MCX-100 Dash Mounted Models

MBD23EXAIJ00K_ MBD43EXAIJ00K_
MBD23EXA7J00K_ MBD43EXA7J00K_

MCX-100 Trunk Mounted Models

MBT23EXAIJ00K_ MBT43EXAIJ00K_
MBT23EXA7J00K_ MBT43EXA7J00K_

The Motorola DES MCX-100 Mobile radios must be purchased with the MBB388 DES option and the MBB39I Security Option. The MBB388 DES coding algorithm module, which replaces the Motorola proprietary DVP algorithm, costs \$103. The MBB39I Security Option - the MBB39IAA for the dash mount model and the MBB39IAB for the trunk mount model - protects the DES and related electronics in a lockable security enclosure and it costs \$283.

The MCX-100 dash mounted mobile radios range in cost from \$2,615 to \$2,895. The MCX-100 trunk mounted mobile radios range in cost from \$2,810 to \$3,090.

FOR OFFICIAL USE ONLY

The Motorola MCX-100 DES Mobile Radios are identified as USGEID 00000012.

13. M/A-COM Linkabit LC76A-DS1

The M/A-COM Linkabit LC76A-DS1 which meets FS-1027 is a bulk encryption device with a Twinax connector which operates at 1.544 megabits/sec in a Bell DS1 data format.

For government applications, the M/A-COM Linkabit LC76A-DS1 requires a KOI-18 key fill device with special cables to load the DES key. The DES key variable must be ordered in a punched paper tape format. Questions concerning the special cables for the KOI-18 should be directed to M/A-COM Linkabit Ken Cohen (619) 457-2340.

NSA has not approved as meeting FS-1027 any Linkabit DES key entry device. Linkabit has chosen not to submit their commercial DES key entry device to NSA for an FS-1027 endorsement.

Cost for the KC76A-DS1 is expected to be in the \$9,000-\$10,000 range.

The following models are endorsed as meeting FS-1027.

LC76A-48VDC-T1-DS1-1PS-1DEU
LC76A-48VDC-T1-DS1-2PS-2DEU
LC76A-48VDC-T1-DS1-2PS-REDUNDANT
LC76A-115VAC-T1-DS1-1PS-1DEU
LC76A-115VAC-T1-DS1-2PS-2DEU
LC76A-115VAC-T1-DS1-2PS-REDUNDANT
LC76A-230VAC-T1-DS1-1PS-1DEU
LC76A-230VAC-T1-DS1-2PS-2DEU
LC76A-230VAC-T1-DS1-2PS-REDUNDANT

All of the above models are assigned USGEID 00000013.

14. M/A-COM Linkabit LC76

The M/A-COM LC-76 is a bulk encryption device which can operate at 1.544 megabits per second or it can be configured to operate on digital data streams from 9600 bits per second to 6 megabits. Keying material requirements and special cable requirements are the same as in number 13.

The LC76 can operate at various input voltages - 115VAC, 230VAC, 48VDC; it can operate with various electrical interfaces - RS442, V35, T1; it can be equipped with one or two power supplies, it can be single channel, dual channel, or 1:1 redundant.

MODEL	<u>INPUT VOLTAGE</u>	<u>ELEC INTERFACE</u>	<u>SYNC FRAMING</u>	<u>POWER SUPPLY REDUNDANCY</u>	<u>DEU REDUNDANCY</u>
LC-76	115VAC	RS442	DS1	1PS	1DEU
	230VAC	V35	gen	2PS	2DEU
	45VDC	T1			REDUNDANT

The LC76 with all possible combinations above are endorsed as meeting FS-1027 and they are identified as USGEID 00000014.

15. Paradyne Info-Lock 1027 Model 2811-03

The Paradyne Info-Lock 1027 Model 2811-03 is a link encryption device that is protocol transparent and can operate in point-to-point or multipoint circuits. This device can operate in the synchronous mode up to 64 KBPS or in the asynchronous mode up to 19.6 KBPS.

Keying variables can be entered into the Paradyne Info-Lock Model 1027 either manually or with a KOI-18. Manual entry requires a printed DES key list. To enter keying variables via a KOI-18, you require special cables and a punched DES key tape. Cables can be ordered from Paradyne.

Cost for the Paradyne Info-Lock 1027 Model 2811-03 is expected to be in the \$2,500 range.

The Paradyne Info-Lock 1027 Model 2811-03 is identified as USGEID 00000015.

16. Racal-Milgo Datacryptor II Model 1027

The Racal Milgo Datacryptor II Model 1027 is a link encryptor/ decryptor which is protocol transparent, half or full duplex and can operate up to 9600 BPS in the synchronous or asynchronous mode.

The Racal-Milgo Datacryptor II Model 1027 requires two keys to operate. The first key to be entered into the equipment is the Initializing Vector and the second key to be entered is the DES keying variable. The Initializing Vector and the DES keying variable must be changed at the same time.

The Initializing Vector and the DES keying variable are entered into the Datacryptor II Model 1027 via a Keywriter. The Keywriter, which is about the size of a hand-held calculator, requires key in a printed tape format.

Cost for the Racal-Milgo Datacryptor II Model 1027 is expected to be in the \$2,500 range.

The Racal-Milgo Datacryptor II Model 1027 is assigned USGEID 00000016.

Date:

Director
National Security Agency
ATTN: S991
Fort George G. Meade, MD 20755

SUBJECT: Telecommunications Protection Bulletin (TPB) Distribution Action Request

1. Type Action Requested:
 - a. _____ Addition to the TPB Distribution List as follows.
 - b. _____ Deletion from the TPB Distribution List as follows.
 - c. _____ Change to the TPB Distribution List as follows. (Company Name/Mailing Address/Company Position/etc. indicated by address label used to mail the TPB to you.)
 - d. _____ Provide copies of previously published TPB's as follows. All _____; Or specific editions (list each edition) _____.
2. Individual's Name:
3. Individual's Position/Title:
4. Division:
5. Company Name:
6. Complete Mailing Address
7. Telephone Number:
8. Number of Copies Requested:

(Signature)

(Printed/Typed Name)

(Company Position/Title)
(If different from Above)

FOR OFFICIAL USE ONLY

NACSI NO.: 6002
DATE: 4 June 1984

National Security Agency

Fort George G. Meade, Maryland



NATIONAL COMSEC INSTRUCTION

PROTECTION OF GOVERNMENT CONTRACTOR TELECOMMUNICATIONS

A9585A. 1-71

Appendix III to TPB Volume I, No. 2, November 1984



NATIONAL SECURITY AGENCY


FORT GEORGE G. MEADE, MARYLAND 20755

4 June 1984

FOREWORD

1. National COMSEC Instruction (NACSI) No. 6002, Protection of Government Contractor Telecommunications, implements three key policies (References a., b., and c.) as they pertain to the telecommunications of Government contractors. Significantly, this NACSI establishes a policy of allowing Government contractors to charge their communications security or protection costs back to the Government in the same manner as they would charge other contract security costs. It requires alternative methods to the present practice of Federal Departments and Agencies providing contractors with Government-Furnished Equipment. This has been a severe burden on the Government's ability to provide adequate communications security equipment for Government contractors.

2. The heads of Federal departments and agencies are responsible for developing procedures to implement this NACSI within their respective organizations. Additional copies of NACSI No. 6002 may be obtained from the Director, National Security Agency, ATTN: S07.


LINCOLN D. FAURER
Lieutenant General, USAF
Director

NACSI No. 6002

1. REFERENCES.

a. REFERENCE DELETED FROM THIS NACSI BEING DISSEMINATED TO GOVERNMENT CONTRACTORS AS APPENDIX III TO TPB, VOLUME I, NO. 2, NOVEMBER 1984

b. NCSC-10, "National Policy for Protection of U.S. National Security-Related Information Transmitted Over Satellite Circuits," dated 26 April 1982.

c. NCSC-11, "National Policy for Protection of Telecommunications Systems Handling Unclassified National Security-Related Information," dated 3 May 1982.

d. REFERENCE DELETED FROM THIS NACSI BEING DISSEMINATED TO GOVERNMENT CONTRACTORS AS APPENDIX III TO TPB, VOLUME I, NO. 2, NOVEMBER 1984

e. REFERENCE DELETED FROM THIS NACSI BEING DISSEMINATED TO GOVERNMENT CONTRACTORS AS APPENDIX III TO TPB, VOLUME I, NO. 2, NOVEMBER 1984

2. PURPOSE. This Instruction provides for the implementation of References a., b., and c. to protect national security and national security-related telecommunications associated with U.S. Government contracts.

3. APPLICABILITY. The provisions of this Instruction apply to the Heads of all Departments and Agencies of the Executive Branch and their contractors.

4. DEFINITIONS.

a. Government Contractor Telecommunications. Telecommunications between or among departments or agencies and their contractors, and telecommunications of, between, or among Government contractors and their subcontractors, of whatever level, which relate to Government business or performance of a Government contract.

b. Government Contractor. An individual, corporation, partnership, association, or other entity performing work under a U.S. Government contract, either as a prime contractor or as a sub-contractor.

5. BACKGROUND. Presently, Government contracts which require exchanges of classified and national security-related information generally obligate the Heads of Federal departments and agencies to provide needed secure equipment as Government-Furnished Equipment (GFE), and the contractors to procure protection equipment at their own expense without direct reimbursement by the Government. The Government's ability to

NACSI No. 6002

satisfy its own operational needs for communications security equipment within currently available inventories tends to place contractors at a disadvantage in competing for these scarce resources. When GFE communications security equipment cannot be made available to and retained by contractors, and they do not opt to procure protection equipment, they must use authorized courier channels, or registered mail, or classified pouch channels (with inherent delays) or make costly and time-consuming visits in order to exchange information.

6. INSTRUCTION. To increase the protection now being given to information transmitted between and among the Government and its contractors, action must be taken to implement the provisions of national policy, as follows:

a. Contract-related telecommunications which require communications security or protection must be identified during the contracting process and specific implementation provisions made for such communications security or protection.

b. Contractors' communications security or protection costs must be allowable in the same manner as they would charge other contract security costs. For applications involving government-provided equipment, this will extend to the associated operating and administrative costs. For applications involving contractor-owned equipment, it will also include associated investment costs.

c. Identify mechanisms by which communications security equipment or approved protection measures can be made directly available to qualified Government contractors in support of national policy and the provisions of this Instruction.

7. RESPONSIBILITIES.

a. The Heads of Departments and Agencies shall establish procedures to:

(1) Identify their contractor telecommunications which require communications security or protection.

(2) Assure that the requirements of this policy are included in the security specifications for each contract.

(3) Assure contractor compliance with those security specifications.

NACSI No. 6002

b. In addition, the Director, National Security Agency shall:

(1) Assist the Heads of Federal Departments and Agencies in assessing threats, vulnerabilities, and risks of exploitation of their contractors' telecommunications.

(2) Recommend alternative mechanisms by which communications security equipment or approved protection measures can be made more readily available to qualified government contractors.

8. IMPLEMENTATION. Classified contractor telecommunications shall be in current compliance with national policy. Unclassified national security-related contractor telecommunications shall be brought into compliance with national policy as soon as possible. Implementation planning shall commence immediately and should be designed to provide protection of contractor telecommunications circuits within two years.

9. EFFECTIVE DATE. This Instruction is effective immediately.