

NACSI NO.: 6002
DATE: 4 June 1984

National Security Agency

Fort George G. Meade, Maryland



NATIONAL COMSEC INSTRUCTION

PROTECTION OF GOVERNMENT CONTRACTOR TELECOMMUNICATIONS

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

1. REFERENCES.

- a. PD/NSC-24, "Telecommunications Protection Policy," dated 16 November 1977.
- b. NCSC-IQ, "National policy for Protection of U.S. National Security-Related Information Transmitted Over Satellite Circuits," dated 26 April 1982.
- c. NCSC-II, "National policy for Protection of Telecommunications Systems Handling Unclassified National Security-Related Information," dated 3 May 1982.
- d. National COMSEC Directive, dated 20 June 1979.
- e. Executive Order 12333, "United States Intelligence Activities" dated 4 December 1981.

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

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.

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.

DISTRIBUTION:

NSA SPECIAL DISTRIBUTION

NSC

DUSD(P) (ATTN: DIR CI&SP and DIR C2 POLICY) (2)

DUSD(C3I) (2)

OJCS (C3I) (2)

CSA (DAMI-CIC) (5)

CNO (3)

CMC (CCT) (5)

CSAF (XOK) (5)

HQ SPACECOM (KR) (2)

CINCLANT (J6) (2)

CINCMAC (DC) (2)

CINCPAC (C3S) (2)

CINCSAC (DC) (2)

USCINCEUR (C3S) (2)

USCINCRD (RCC4S) (2)

USCINCSO (J6) (2)

USCINCCENT (CCJ6) (2)

COMUSFCARIB (J6) (2)

COMUSJAPAN (J6) (2)

COMUSKOREA (J6) (2)

DIR TRI-TAC (TT-SC) (2)

DIR TRI-TAC JTE (TT/TE-C)

CDR USAINSCOM,

(IAOPS-OP-P) (15)

COMNAVSECGRU (G-61) (15)

COMNAVTELCOM (Code 1243) (5)

DCMS (T30) (3)

CGMCDEC (DEVGEN C3) (2)

AFCSC (EPPP) (5)

DCA (Code B315) (20)

DIA (RCM-4)

DLA (DLA-TI) (2)

DNA (LECD) (2)

Dept. of Agriculture

(MSD/FAS) (2)

Dept. of Commerce (I&S) (2)

Dept. of Energy (CSTM) (2)

Dept. of Health & Human Svcs (IG) (2)

Dept. of Interior (AMO) (2)

Dept. of Justice (SPS JMD) (2)

Dept. of State (ASC) (2)

Dept. of Transportation

(Security Staff, M-441) (2)

Dept. of Treasury (ADTM) (10)
CIA (OC-CSD) (2)
FAA (ACS300) (2)
FCC (Code 22800) (2)
FBI (TSD) (2)
FEMA (RMIR-IM-TW-CS) (7)
GSA (Code KJS) (2)
NASA (NIS-S) (2)
NCS (AO) (2)
NRC (DS 286-SS) (2)

cc: C/S
EX REG
DDA
DDC
DDO
DDPP
DDT
DDX
ADT
GC (3)
IG (3)
Chief, C
FIA
FIB
FIC
FID
FIE
FIF
FIG
FIH
FII
FIJ (3)
FIK
FIL
FIM
F2 (5)
F23
F24
F31
F32
F321
F33
F34
F38
F4 (5)
F41
F45
F47
F6
F71
F8
F81 F83 F91
F92
F92 (Vital Records) F93
L221
NSALO/DCA

NSALO/TRI-TAC
NSALO/TRI-TAC JTE
P2
Q1
Q4
U5COMSEC EXPERT TO NICSMA
S011 (20)
S011 (History File) .
S02
S04 (2)
S07
S08
S071 (30)
S072
S073
S1 (2)
S2
S3
S4
S5
S6
S7
S8
S9
T09
T1
T11
T2
T3
T4