356633
ZL T001
ND011
PR
FG006
FG038
FG006-11
FG006-14
FG006-12
FG013-10
FG006-03
FG006-21
FG013-01

THE WHITE HOUSE

WASHINGTON 3240

April 22, 1986

MEMORANDUM FOR RICHARD RILEY
CHRISTOPHER HICKS

FROM: JOHN M. POINDEXTER for

SUBJECT: Protection of Government Contractor Telecommunications - NACSI No. 6002

National Communications Security Instruction (NACSI) No. 6002, "Protection of Government Contractor Telecommunications," provides guidance allowing Government Contractors to charge their communications security or protection costs back to the Government in the same manner as they would charge other contractor security costs.

The National Manager, National Telecommunications and Information Systems Security (NTISS) (Tab A) has extended the implementation date of NACSI No. 6002 to December 31, 1986. In view of the responsibilities of your office for contracting and providing telecommunications services for Executive Office of the President (EOP) organizations on the White House Complex and in the National Capital Region, it is requested that your respective offices conduct a joint survey of COMSEC requirements for contractor telecommunications and provide a detailed implementation schedule to the National Manager as outlined in Tab A. The National Security Agency (NSA) will provide technical assistance as required to conduct the survey.

Attachment
Tab A Memorandum from National Manager

cc: Office of the Vice President
Office of Management and Budget
Office of Science and Technology Policy
NSC/Situation Room/CMC
U.S. Secret Service
Council of Economic Advisers
PFIAB
National Manager, NTISS (Director, NSA)

NSC #8603240

Lt. Gen. William E. Odom

**NTISS**
NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

# NATIONAL MANAGER

NTISS-003/86
14 March 1986

MEMORANDUM FOR DISTRIBUTION

SUBJECT: NACSI No. 6002 Compliance

1. National Communications Security Instruction (NACSI) No. 6002, "Protection of Government Contractor Telecommunications," dated 4 June 1984 (attached), requires implementation of protection for government contractor telecommunications circuits by 4 June 1986. This memorandum extends that date to 31 December 1986. This extension is in large part due to unforeseen problems in putting into place the necessary mechanisms to allow compliance.

2. NACSI No. 6002 requirements for secure and protected contractor telecommunications will vary among federal departments and agencies. These requirements may be determined to be for the STU-II or STU-III secure voice equipment, for existing voice and data encryption gear such as the KG-84, for other Controlled Cryptographic Items (CCI) equipment, or for other NSA-endorsed equipment or protected services. Secure equipment or protected services must be purchased by 31 December 1986, or in cases in which STU-III secure voice equipment is determined to meet the protection requirement, funded orders for the STU-III must be received at the National Security Agency or by an authorized STU-III vendor by 31 December 1986.

3. Departments and agencies are further requested to provide a detailed implementation schedule for protection of their contractor telecommunications by 31 March 1987.

Wm E Odom

WILLIAM E. ODOM
Lieutenant General, USA

Encl:
a/s

Copy Furnished:
Executive Agent, NTISS
ASC ($C^3I$)
NSC
NTISSC Secretariat

Serial: NTISS-003/86

DISTRIBUTION:

Secretary of State
Department of State 2201 C Street, N.W.
Washington, D.C. 20520

Secretary of Treasury
Department of Treasury
15th Street and Pennsylvania Ave, N.W.
Washington, D.C. 20220

Attorney General of the United States
Department of Justice
Constitution Ave and
Tenth Street, N.W.
Washington, D.C. 20530

Secretary of Interior
Department of the Interior
C Street between Eighteenth
and Nineteenth Street, N.W.
Washington, D.C. 20240

Secretary of Agriculture
Department of Agriculture
Fourteenth Street and
Independence Ave, S.W.
Washington, D.C. 20250

Secretary of Commerce
Department of Commerce
Fourteenth Street between
Constitution Ave & E St., N.W.
Washington, D.C. 20230

Secretary of Labor
Department of Labor
200 Constitution Ave, N.W.
Washington, D.C. 20210

Secretary of Health and
Human Services
Department of Health and
Human Services
200 Independence Ave, S.W.
Washington, D.C. 20201

Secretary of Housing and
Urban Development
Department of Housing and
Urban Development
451 Seventh St., S.W.
Washington, D.C. 20410

Secretary of Transportation
Department of Transportation
400 Seventh Street, S.W.
Washington, D.C. 20410

Secretary of Energy
Department of Energy
1000 Independence Ave, S.W.
Washington, D.C. 20585

Secretary of Education
Department of Education
400 Maryland Ave, S.W.
Washington, D.C. 20202

Director
Office of Management and Budget
Executive Office Building
Washington, D.C. 20503

Director
Central Intelligence Agency
Washington, D.C. 20505

Acting Administrator
General Services Administration
General Services Building
Eighteenth and F Streets, N.W.
Washington, D.C. 20405

Director
Federal Emergency Management Agency
500 C Street
Washington, D.C. 20472

Manager
National Communications System
18th & South Courthouse Road
Arlington, Virginia 22204

Chairman
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

Administrator
National Aeronautics and
Space Administration
400 Maryland Ave, S.W.
Washington, D.C. 20546

Chairman
Nuclear Regulatory Commission
1717 H Street, N.W.
Washington, D.C. 20555

Administrator
Federal Aviation Administration
800 Independence Ave, S.W.
Washington, D.C. 20591

National Bureau of Standards
Washington, D.C. 20234

Director
United States Information Agency
400 C Street, S.W.
Washington, D.C. 20547

Manager
White House Communications Agency
National Communications System
8th and South Courthouse Road
Washington, D.C. 22204

Comptroller General
of the United States
General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Commandant of the Marine Corps
Code INTS
Headquarters, Marine Corps
Washington, D.C. 20380

Commander
Naval Security Group Command
U.S. Naval Security Group Headquarters
3801 Nebraska Avenue, N.W.
Washington, D.C. 20390

Director
Defense Intelligence Agency
The Pentagon
Washington, D.C. 20301

Director
Defense Logistics Agency
Cameron Station
Alexandria, Virginia 22314

Director
Defense Nuclear Agency
Washington, D.C. 20305

Director
Federal Bureau of Investigation
Tenth & Pennsylvania Ave, N.W.
Washington, D.C. 20535

Chairman
Joint Chiefs of Staff
The Pentagon
Washington, D.C. 20301

Chief Naval Operations
Department of the Navy
The Pentagon
Washington, D.C. 20305

USAF Special Security Office
AFIS/INSD
The Pentagon, Room BD951
Washington, D.C. 20301

Special Security Office
HQ ADCOM/INXS
Peterson Air Force Base, CO. 80914-5001

Commander in Chief
U.S. Atlantic/Atlantic Fleet
U.S. Naval Base
Norfolk, VA 23511
ATTN: SCI Branch (N26)

HQ MAC/INS
Scott AFB, IL 62225

Special Security Office
USCINCPAC
Box 42
Camp H.M. Smith, Hawaii 96861-5025

Special Security Office
544 IES/IEE
Offutt AFB, NE 68113

Commander in Chief
U.S. European Command
ATTN: C3S
APO New York, N.Y. 09128

Special Security Office
TO BE OPENED ONLY BY SSO
USREDCOM RM 207, Bldg 501
MacDill AFB, FL 33608-6001

Chief, SSO/SPINTCOMM DIV
J-2 Directorate
USSSOUTHCOMM
APO Miami 34003

Commander in Chief
U.S. Central Command
ATTN: CCJ6-C
MacDill Air Force Base, FL 33608-7001

Commander
U.S. Forces Caribbean
P.O. Box 9058
Key West, Florida 33040-6300

5 AF/INS
TO BE OPENED ONLY BY: AFSSO/INS
APO San Francisco 96328

Commander
USASSD ACSI DA
HQA
UNC/CFC/USFK/EUSA
APO San Francisco 96301

Commander
Joint Test Element
Joint Tactical Communications
(TRI-TAC) Office
Fort Huachuca, AZ 85613

Commander
U.S. Army Intel & Sec Command
Arlington Hall Station
Arlington, Virginia 22212

COMNAVTELCOM (913)
4401 Massachusetts Avenue
Washington, D.C. 20390

Director
COMSEC Material System
3801 Nebraska Avenue, N.W.
Washington, D.C. 20390

Commanding General
Marine Corps Development
and Education Command
ATTN: DEVCEN C3
Quantico, VA 22134

NACSI NO.: 6002
DATE: 4 June 1984

# National Security Agency

**Fort George G. Meade, Maryland**

NATIONAL COMSEC INSTRUCTION

PROTECTION OF GOVERNMENT CONTRACTOR TELECOMMUNICATIONS

Enclosure

A9585A. 1-71

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-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. 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.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

ACTION

April 21, 1986

MEMORANDUM FOR JOHN M. POINDEXTER

FROM: JOHN G. GRIMES/KENNETH E. DEGRAFFENREID

SUBJECT: Protection of Government Contractor Telecommunications for EOP Organizations (NACSI No. 6002)

NACSI No. 6002, "Protection of Government Contractor Telecommunications," issued by the Director, NSA, provides guidance to Federal Agencies and Departments allowing the Government Contractors to charge their communications security or protection costs back to the Government in the same manner as they (contractors) charge other contract security costs. This policy guidance was issued to encourage Federal Agencies and Departments to protect sensitive information that is handled by Government Contractors. The National Manager, NTISS, at Tab A, has extended NACSI No. 6002 to December 31, 1986, and requested agencies to identify their COMSEC requirements for protection by Government Contractor telecommunications. The National Manager also requested an Agency detailed implementation plan for accomplishing this protection by March 31, 1987.

Office of Administration (OA) and White House Communications Agency (WHCA) provide primarily telecommunications services/ support to EOP organizations on the White House Complex and the National Capital Region. In view of these dual responsibilities OA and WHCA are being asked (Tab I) to conduct a joint survey of COMSEC requirements for contractor telecommunications and provide a detail implementation schedule to the National Manager (Tab A). This request falls within the purview of NSDD-113, "Security of Communications Systems Used by Key Government Officials" which assigns you the responsibilities for determing the users and priority of implementation of telecommunications systems.

RECOMMENDATION

That you sign the Memorandum (Tab I) to Chris Hicks and Rick Riley requesting they conduct a joint survey of COMSEC requirements for protection of contractor telecommunications and to provide the National Manager an implementation plan.

Approve _____ Disapprove _____

Attachments

Tab I Memorandum to Chris Hicks & Rick Riley
Tab A Memorandum from National Manager

SYSTEM II
90944

THE WHITE HOUSE

WASHINGTON

January 22, 1988

NATIONAL SECURITY DECISION
DIRECTIVE NUMBER 298

# NATIONAL OPERATIONS SECURITY PROGRAM

## OBJECTIVE

Security programs and procedures already exist to protect classified matters. However, information generally available to the public as well as certain detectable activities reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions in the area of national security. Application of the operations security (OPSEC) process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.

## OPSEC PROCESS

The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified activity could be acquired in light of the known collection capabilities of potential adversaries. Such evidence usually derives from openly available data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators most often stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. Once identified, they are analyzed against the threat to determine the extent to which they may reveal critical information. Commanders and managers then use these threat and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.

OPSEC thus is a systematic and proved process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.