DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

OPNAVINST 2221.5C
N6
7 Feb 07

OPNAV INSTRUCTION 2221.5C

From: Chief of Naval Operations

Subj: RELEASE OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL TO U.S. INDUSTRIAL FIRMS UNDER CONTRACT TO THE U.S. NAVY

Ref: (a) DOD Manual 5220.22-M (National Industrial Security Program Operating Manual, January 1995 and Supplements)
(b) DOD Supplement 5220.22-S-1 (COMSEC Supplement to the Industrial Security Manual for Safeguarding Classified Information) of March 1998 (NOTAL)

1. Purpose. To revise policy and expand procedures for authorizing release of COMSEC material to U.S. industrial firms under contract to the U.S. Navy.

2. Cancellation. OPNAVINST 2221.5B.

3. Applicability. The following terms are defined as applicable to this instruction:

a. COMSEC material - Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to: key, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

b. COMSEC equipment - Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, crypto-production equipment, and authentication equipment.

4. Policy. Government cryptographic equipment operations will ordinarily be conducted by the Government. However, when there is a valid need and it is clearly in the best interest of the Navy and the Government, cryptographic equipment, keying material, related COMSEC information, and access to classified U.S. Government traffic may be provided to U.S. contractors to:

a. Install, maintain, or operate "TSEC" nomenclatured COMSEC equipment or controlled cryptographic item (CCI) for the U.S. Government.

b. Participate in the design, planning, production, training, installation, maintenance, operation, logistical support, integration, modification, testing, or study of COMSEC material or techniques.

c. Electrically communicate classified national security information in a cryptographically secure manner, or unclassified national security-related information by COMSEC protected means.

5. Requirements. Contractor personnel who are granted access to COMSEC material must be U.S. citizens. Such access shall be controlled on a strict need-to-know basis and shall be granted only in conformance with procedures established for the particular type of COMSEC information involved. Detailed guidance for contracting offices concerning security clearances, access authorization, and briefings are set forth in references (a) and (b). All contracts involving COMSEC material with industrial firms must contain the following information:

a. U.S. cryptographic equipment inventory information, as well as the systems and manner in which each particular equipment is used, is for official use only. Publication or release of any related COMSEC information by any means, by the commercial firm, without prior written approval of the contracting office is prohibited.

b. Individuals granted access to classified COMSEC material must hold a final Government security clearance for the level of classification involved. The clearances of facility security officers, COMSEC custodians, and alternate COMSEC custodians must be predicated on a favorable background investigation current within five years.

c. All individuals provided access to COMSEC material must be briefed at least annually regarding the unique nature of COMSEC material and their security responsibilities to safeguard and control it.

d. All individuals who maintain Government cryptographic equipment or CCI must receive formal NSA-approved training on such equipment.

6. Action. Prior to release of any COMSEC material to a U.S. industrial firm under contract to the U.S. Navy for one of the purposes describe in paragraph 4, the contracting office shall submit a request to the Commander, Naval Network Warfare Command (COMNAVNETWARCOM) for review and approval. Provide copies to the Chief of Naval Operations (N6F3) and COMSEC Material System (NCMS). The request shall include sufficient justification upon which to base a decision that such release is in the best interest of the Navy and the Government and a statement that all applicable requirements of this instruction and references (a) and (b) have been met. Additionally, the following applicable information shall be included in the request:

a. Contract number, name of contractor, licensee, or individual; facility clearance; and location at which the functions will be performed

b. Nature and scope of the contractual functions; the COMSEC material or cryptographic equipment to which the contractor personnel will have access; and the number of contractor personnel involved.

c. In the case of contractor operation of a secure telecommunications facility, the classification and type of material involved and whether access to U.S. Government traffic will be supervised by government civilian or military personnel.

d. The initial date on which contractor personnel will have access to COMSEC material or equipment and the length of the contract or period of time such access will be required.

e. Description of any additional administrative or security measures over and above the requirements of this instruction or of references (a) and (b), which will be implemented to ensure that contractor personnel will not gain access to classified

information or material for which they do not possess a security clearance and valid need-to-know.

7. Accounts. COMSEC accounts established at contractor facilities in accordance with reference (b), as a result of Navy contracts, are NSA accounts administered by the Director, National Security Agency (DIRNSA). NCMS will assist in establishing COMSEC accounts as necessary.

8. Approval. COMNAVNETWARCOM shall review each request received to ensure that all the requirements of the national policy for release of COMSEC material to U.S. industrial firms are fulfilled; approve the release from a national policy aspect; and advise appropriate commands and the DIRNSA of the approval so that other required action can be initiated. In the event the provisions of this instruction cannot be met and sufficient justification for release to contractor personnel is provided, COMNAVNETWARCOM will initiate action to request an exception to the national policy from the Committee on National Security Systems (CNSS). The following checklist should be used as a guideline in requesting exceptions to this policy:

a. Identify the individual and/or organization, their citizenship, their level of security clearance, and the location(s) at which COMSEC functions will be performed.

b. Identify the COMSEC functions the nongovernment sources(s) will perform, the COMSEC material to which the individual(s) will have access, the number of personnel involved, their training certification or any training required.

c. List the classification of the COMSEC material to which the source personnel will have access.

d. Indicate whether source personnel will be using keying materials marked "CRYPTO" which are held or used by Government departments and agencies. If so, has consideration been given to providing unique operational keying materials?

e. Indicate what additional administrative/security measures will be implemented.

f. Identify the inclusive dates for which source personnel will have access to COMSEC material under the provision of the contract or arrangement.

g. Identify the Government department or agency which will be responsible for assuring the security of nongovernment cryptographic operations/functions.

h. Identify the specific provisions of this instruction for which an exception is required.

9. Continuing Action. COMNAVNETWARCOM shall be kept informed for the life of the contract of any events that affect the length of the contract or the type and amount of COMSEC material involved. COMNAVNETWARCOM shall also be notified of the date of the actual termination of the contract.

M. J. EDWARDS
Vice Admiral, U.S. Navy
Deputy Chief of Naval Operations
(Communication Networks) (N6)

Distribution:
Electronic only, via Department of the Navy Issuances Website
http://doni.daps.dla.mil