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

OPNAVINST 2221.5D
N2N6
15 Aug 2016

OPNAV INSTRUCTION 2221.5D

From: Chief of Naval Operations

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

Ref: (a) DON CIO Guidance on Information Management/Information Technology Inherently Governmental, 1 Nov 2001 (NOTAL)
(b) DoD 5220.22-M, National Industrial Security Program Operating Manual, February 2006
(c) CNSSI 4000, Maintenance of Communications Security Equipment, 12 Oct 2012 (NOTAL)
(d) DoD 8570.01-M, Information Assurance Workforce Improvement Program, December 2005
(e) Electronic Key Management System 1 (EKMS 1B) of 5 April 2010 (NOTAL)

1. Purpose. To publish procedures for authorizing the release of communications security (COMSEC) material to U.S. industrial firms under contract to the Department of the Navy (DON). This revision updates references and incorporates current requirements for the handling of COMSEC information, materials, and equipment as well as responsibilities of the information assurance workforce. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 2221.5C.

3. Definitions

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, or other items that perform COMSEC functions.

b. COMSEC Equipment. Equipment designed to provide security to telecommunications by encrypting data for

transmission and decrypting data for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process.

4. Policy. Per reference (a), management of cryptographic material, equipment, and COMSEC operations are considered an inherently governmental function. However, when there is a valid need and such is clearly in the best interest of the DON and the U.S. Government, cryptographic equipment, keying material, related COMSEC information, and access to classified U.S. Government information may be provided to U.S. contractors to:

a. Install, maintain, or operate transmission security nomenclature COMSEC equipment or controlled cryptographic items (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. Electronically communicate classified national security information in a cryptographically secure manner, or unclassified national security-related information by COMSEC protected means.

5. Requirements. Contractor personnel granted access to COMSEC material must be U.S. citizens and possess a valid security clearance. Such access must be controlled on a strict need-to-know basis and granted only in conformance with procedures established for the particular type of COMSEC material and equipment involved. Detailed guidance for contracting offices concerning security clearances, access authorization, and briefings is set forth in reference (b). All contracts involving COMSEC material with industrial firms must contain the information in subparagraphs 5a through 5e.

a. U.S. cryptographic equipment inventory information and the systems and applications used are for official use only. Publication, disclosure, or other release of COMSEC related information by any means by a contracting entity without prior written approval of the contracting office is prohibited.

b. Contractor personnel granted access to classified COMSEC material must hold a final personnel security clearance appropriate for the COMSEC material accessed. Clearances for facility security officers, COMSEC custodians, and alternate COMSEC custodians having access to top secret keying material marked as containing cryptographic information must have a final security clearance based upon a single scope background investigation current within 5 years.

c. All contractor personnel with access to COMSEC material must be briefed annually regarding the unique nature of COMSEC material and their responsibilities for safeguarding and controlling the material.

d. Contractor personnel who perform maintenance on U.S. Government cryptographic equipment or CCI must satisfy and comply with the provisions of reference (c).

e. Per reference (d), chapters 2 and 3, contractor personnel, whose duties require privileged access to a government computer system, including those used for COMSEC management purposes must be trained and certified.

6. Action

a. Prior to release of any COMSEC material or COMSEC related information to a U.S. industrial firm under contract to the DON for one of the purposes described in paragraph 4, the contracting office must submit a request to Naval Communications Security Material System (NCMS) for review, validation, and recommendation for approval on behalf of Commander, Navy Information Forces (COMNAVIFOR). The request must include sufficient justification upon which to base a decision and indicate that the release is in the best interest of the DON and U.S. Government. Additionally, the request must include a statement that all applicable requirements of this instruction and the references contained herein have been met.

b. Upon approval, NCMS will notify the requestor and provide the assigned contract authorization number, which will expire at the end of the contract. All subsequent correspondence related to COMSEC material or COMSEC related information must include the contract authorization number assigned. Upon approval, if granted, the vendor may request

COMSEC material or COMSEC related information, as applicable per reference (e) citing the contract authorization number as the supporting authorization. The request must include, at a minimum those listed in subparagraphs 6b(1) through 6b(5).

(1) Contract number; name of contractor; licensee or individual; facility clearance; and location where the functions will be performed.

(2) 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.

(3) In the case of a contractor's operation in a secure telecommunications facility: the classification and type of material involved, and whether access to U.S. Government message traffic or related information will be supervised by government civilian or military personnel.

(4) 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.

(5) Any other information deemed appropriate in evaluating the request.

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

8. Policy Exception Approval. In the event the provisions of this instruction cannot be satisfied and sufficient justification for release of COMSEC material or COMSEC related information to contractor personnel is provided, NCMS, in collaboration with COMNAVIFOR and the NSA will initiate necessary action(s) to request an exception from DON Chief Information Officer. The checklist in subparagraphs 8a through 8h 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 non-government 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 in which the source personnel will have access.

d. Indicate whether personnel will be using keying material marked "CRYPTO" held or used by government departments and agencies. If so, state whether consideration has been given to providing unique operational keying materials.

e. Indicate additional administrative and security measures which will be implemented.

f. Identify the inclusive dates personnel will have access to COMSEC material under the provision of the contract.

g. Identify the government department or agency which will be responsible for the security of non-government cryptographic operations and functions.

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

9. Continuing Action. COMNAVIFOR and NCMS must be kept informed throughout the life of the contract on any events that affect the length of the contract or the type and amount of COMSEC material involved. COMNAVIFOR and NCMS must also be notified of the date of the actual termination of the contract.

10. Review and Effective Date. Per OPNAVINST 5215.17A, Deputy Chief of Naval Operations, Information Warfare (CNO N2N6) will review this instruction annually on the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy (SECNAV), and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will

automatically expire 5 years after its issuance date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

11. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV Manual 5210.1 of January 2012.

JAN E. TIGHE
By direction

Distribution:
Electronic only, via Department of the Navy Issuances Web site
http://doni.documentservices.dla.mil/