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

OPNAVINST 2201.3B
N6
14 Apr 09

OPNAV INSTRUCTION 2201.3B

From: Chief of Naval Operations

Subj: COMMUNICATIONS SECURITY MONITORING OF NAVY TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY SYSTEMS

Ref: (a) NTISSD No. 600 of 10 Apr 90 (NOTAL)
(b) DoD Instruction 8523.01 of 22 Apr 08
(c) DoD Instruction 8560.01 of 09 Oct 07

Encl: (1) COMSEC Monitoring Terms and Definitions
(2) Procedures for COMSEC Monitoring of Telecommunications and IT Systems

1. Purpose. To issue general policy and procedures governing Communications Security (COMSEC) monitoring within the Navy. This instruction has been administratively revised and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 2201.3A.

3. Application. The provisions of this instruction apply to all Navy commands and components.

4. Scope

a. This instruction establishes authority for implementing COMSEC monitoring in the Navy and addresses responsibilities necessary for compliance with references (a), (b), and (c). Specifically, this instruction governs monitoring of Navy organizational and personal communications equipment, telephone, and Information Technology (IT) systems equipment.

b. This instruction does not pertain to:

(1) Systems administration/management functions to ensure proper installation, integration and functioning of equipment and systems, including local security devices and systems.

(2) Signals intelligence, Foreign Intelligence (FI) and Counterintelligence (CI) collection activities.

(3) Interception of communications for law enforcement purposes.

5. Policy

a. The Navy will conduct, and allow other non-Navy organizations to conduct, COMSEC monitoring activities only as necessary to determine the degree of security provided to telecommunications and IT systems and aid in countering their vulnerability to interception, technical exploitation, the human intelligence threat, and other dimensions of the FI threat. Such activities shall be conducted in strict compliance with law, Executive orders, applicable Presidential directives, and references (a) through (c). Only authorized personnel assigned to Navy Information Operations Command Norfolk, Navy Cyber Defense Operations Command, or other commands authorized by Commander, Navy Network Warfare Command (COMNAVNETWARCOM), as the Navy's designated service cryptologic element, will conduct activities such as red/blue team operations or other activities that would constitute COMSEC monitoring under the auspices of the current definition. The Director, National Security Agency (DIRNSA) under the authority, direction, and control of the Under Secretary of Defense for Intelligence serves as the Department of Defense (DoD) focal point for COMSEC monitoring. DIRNSA provides COMSEC monitoring services to the Navy through the Joint COMSEC Monitoring Activity (JCMA), when requested, in accordance with reference (a). When COMSEC monitoring is requested by a non-Navy entity for which Navy is the executive agent (e.g., Pacific Command, Secretary of the Navy (SECNAV)), monitoring services are provided to the non-Navy entity through the JCMA.

b. The prohibitions of paragraphs 14, 15, 17, 18, 22, and 23 of reference (a) set forth certain restrictions and prohibitions on monitoring activities. These apply to Navy COMSEC monitoring activities covered by this instruction, specifically:

(1) Government telecommunications systems are subject to COMSEC monitoring by duly authorized government entities;

(2) Users of these systems must be properly notified in advance that their use of these systems constitutes consent to monitoring for COMSEC purposes;

(3) The Government will not monitor systems which are owned or leased by government contractors without first obtaining approval of the company chief executive officer and notifying employees;

(4) The Government shall not monitor, for COMSEC purposes, the content of any telecommunications when such monitoring would constitute electronic surveillance;

(5) The results of COMSEC monitoring shall not be used to produce FI or CI;

(6) No service department or government agency may monitor the telecommunication of another department or agency for COMSEC purposes without the approval of the department or agency to be monitored;

(7) No incidentally acquired nonpublic communication may be monitored beyond a point at which a determination can reasonably be made that it is nonpublic; and

(8) Contents of any nonpublic communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a government communication.

c. In accordance with procedures approved by the Attorney General of the United States, information acquired incidentally from government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction. For the purpose of this instruction, a crime shall be considered "significant" if it is a "major criminal offense" as defined by SECNAVINST 5430.107. When taking such action, the General Counsel of the Navy will be notified promptly. The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the General Counsel of the Navy.

d. COMSEC monitoring shall be authorized only:

(1) When the General Counsel of the Navy has determined that sufficient notice has been given to Navy users. If the biennial written determination made by the General Counsel of the Navy has lapsed and an emergent need to conduct COMSEC monitoring is identified, an echelon II commander's judge advocate or general counsel can provide a written notification of such determination for the distinct and emergent COMSEC monitoring event;

(2) When it will aid in protecting national security as described in subparagraph 5a; and

(3) When the period of monitoring is for 1 year or less.

e. This instruction combines with periodic notices and reminders (issued by an All Navy Message (ALNAV)) to serve as notification of Navy intent to monitor official communications of Navy commands and staff. Notification of specific COMSEC monitoring operations is not required.

f. Navy COMSEC monitoring activities shall be consistent with paragraphs 20 and 25 through 30 of reference (a) with respect to monitoring procedures; acquisition, retention and storage procedures; dissemination procedures; and safeguarding of monitoring equipment.

6. Responsibilities

a. The Chief of Naval Operations (CNO) will:

(1) Advise the General Counsel of the Navy of the actions taken within the Navy to notify users of official DoD telecommunications systems and IT systems that such systems are subject to COMSEC monitoring at all times and that use of such systems constitutes consent to COMSEC monitoring.

(2) Approve instructions and procedures for the proper conduct of COMSEC monitoring within the Navy.

b. Fleet Commanders (FLTCDR) will:

(1) Approve COMSEC monitoring requests and direct COMSEC monitoring operations for Navy commands under their operational or administrative control. Navy commands not under control of a FLTCDR will request COMSEC monitoring operations from COMNAVNETWARCOM.

(2) Provide notice to COMNAVNETWARCOM by 1 July of even-numbered years that each of the commands under their operational or administrative control have complied with the requirement to notify users of official DoD telecommunications systems and IT systems that such systems are subject to COMSEC monitoring at all times and that use of such systems constitutes consent to COMSEC monitoring. Navy commands not under control of a FLTCDR will notify their echelon II commander of the same compliance, and those echelon II commanders will provide notice to COMNETWARCOM by 1 July of even-numbered years.

c. COMNAVNETWARCOM will:

(1) Approve specific COMSEC monitoring operations for commands outside a FLTCDR operational chain.

(2) Compile the information supplied in accordance with subparagraph 6b(2) above and forward to the CNO for use in advising the General Counsel of the Navy's compliance with the notification and consent requirements.

(3) Provide CNO advice and assistance on the conduct of COMSEC monitoring activities and procurement of COMSEC monitoring equipment for use by Navy commands.

(4) Conduct liaison with the National Security Agency and JCMA to ensure Navy compliance with national COMSEC monitoring directives.

(5) Ensure personnel are properly trained for the conduct of COMSEC monitoring activities conducted by Navy activities listed in subparagraph 5a above.

(6) Act as the certifying authority for all Navy personnel and commands conducting COMSEC monitoring.

(7) Oversee training and provide the required certifications for all Navy commands designated to conduct

COMSEC monitoring. COMSEC monitoring may be undertaken only for the purposes enumerated in paragraph 20 of reference (a).

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed in accordance with SECNAV Manual 5210.1.

8. Definitions and Procedures. Enclosures (1) and (2) provide definitions of COMSEC monitoring terms and procedures for conducting COMSEC monitoring of telephones, facsimile machines, cellular telephones, organizational and personal communications equipment, and IT systems equipment.

9. Form. DD 2056 (5/00), Telephone Monitoring Notification Decal, is available on Naval Forms OnLine https://navalforms.daps.dla.mil/web/public/home.

Example: "DO NOT DISCUSS CLASSIFIED INFORMATION. THIS TELEPHONE IS SUBJECT TO MONITORING AT ALL TIMES. USE OF THIS TELEPHONE CONSTITUTES CONSENT TO MONITORING".

HARRY B. HARRIS, JR.
Vice Admiral, U.S. Navy
Deputy Chief of Naval Operations
(Communication Networks)(N6)

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

COMSEC MONITORING TERMS AND DEFINITIONS

1. Information Technology (IT) Systems. Any equipment or interconnected systems or subsystems of equipment, including computer software, firmware, and hardware, that are used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.

2. COMSEC (Communications Security). Protective measure taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including crypto security, transmission security, emissions security, password management and file protection) to telecommunications systems and IT systems which generate, handle, process, store, or use classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes the application of physical security measures to COMSEC information or materials.

3. COMSEC Monitoring. The act of listening to, copying, or recording transmissions and data processing of one's own official telecommunications and IT systems to provide material for analysis in order to determine the degree of security being provided to those transmission and data processes. For the purpose of this instruction, COMSEC monitoring includes all activities involving remote access to IT systems by non-local system administrators to include, but not limited to, on-line surveys, red team operations, and naval computer incident response team duties.

4. Electronic Surveillance. The acquisition of the contents of a nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

5. Telecommunications. The transmission, communication, or processing of information, including the preparation of such

information by electrical, electromagnetic, electromechanical, or electro-optical means.

6. Telecommunications Systems. The interconnected devices used to transmit and/or receive communications or process telecommunications; the devices may be electrical, electromagnetic, electromechanical, or electro-optical.

7. Telephone Monitoring. That portion of COMSEC monitoring which deals specifically with telephones.

8. Organizational Communications Equipment. All unclassified government equipment patched through the Naval Computer and Telecommunications Area Master Station (NCTAMS).

9. Personal Communications Equipment. All unclassified government equipment patched through the NCTAMS.

PROCEDURES FOR COMSEC MONITORING OF TELECOMMUNICATIONS AND IT SYSTEMS

1. Request

a. Individual commands/commanders submit requests for conduct of COMSEC monitoring of Navy telecommunications and IT systems via their operational chain of command to the appropriate FLTCDR.

b. Navy echelon II commanders or commanders outside FLTCDR chain of command may submit requests for conduct of COMSEC monitoring of their own or subordinates' Department of the Navy telecommunications systems and IT systems to COMNAVNETWARCOM.

2. Notification. Commanding officers/unit commanders are responsible for ensuring the following notification is provided to their subordinates. Such notification, in addition to this instruction, constitutes sufficient notification to conduct COMSEC monitoring operations.

a. Users of official DoD telecommunications systems and IT systems shall be notified that discussion/transmission of classified information over non-secure circuits is prohibited; that official DoD telecommunications systems and IT systems are subject to COMSEC monitoring at all times; and that use of such telecommunications systems and IT systems constitutes consent to COMSEC monitoring. Additionally, the above information must be included in orientation briefings.

b. Proper notification should also include quarterly notices in the daily bulletin or Plan of the Day, specific memoranda to users, periodic training programs, and a statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

c. All non-secure telecommunications devices will have decals (DD 2056) attached to the lower front portion.

d. All official Navy non-secure telecommunications devices will have this information prominently displayed on their covers in the following format:

"DO NOT DISCUSS CLASSIFIED INFORMATION - THIS TELEPHONE IS SUBJECT TO MONITORING AT ALL TIMES. USE OF THIS TELEPHONE CONSTITUTES CONSENT TO MONITORING." DoD telephones are provided for the transmission of official government information and are subject to communications security monitoring at all times. Use of official DoD telephones constitutes consent to communications security telephone monitoring in accordance with reference (a).

e. All official Navy IT systems are required to display the legally approved logon warning banner as defined in DoD Memorandum of 9 May 2008, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," which also serves to provide notification of, and consent to, COMSEC monitoring.