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

OPNAVINST 2201.3A
N6
2 Aug 07

OPNAV INSTRUCTION 2201.3A

From: Chief of Naval Operations

Subj: COMMUNICATIONS SECURITY (COMSEC) MONITORING OF NAVY TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS (AIS)

Ref: (a) NTISSD No. 600 of 10 Apr 90 (NOTAL)
(b) DOD Directive C-5200.5 of 21 Apr 90 (NOTAL)
(C) DOD Directive 4640.6 of 26 Jun 81

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

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

2. Cancellation. OPNAVINST 2201.3

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

4. Scope

a. This instruction establishes authority for implementing Communications Security (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 automated information systems (AIS) 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 (SIGINT), foreign intelligence, and counter-intelligence collection activities.

(3) Interception of communications for law enforcement purposes.

5. Policy

a. The Navy will conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to telecommunications and AIS and aid in countering their vulnerability to interception, technical exploitation, the human intelligence (HUMINT) threat, and other dimensions of the foreign intelligence threat. Such activities shall be conducted in strict compliance with law, Executive Orders, applicable Presidential Directives, and references (a) through (c).

(1) Fleet Commanders (FLTCDR) will approve COMSEC monitoring request 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 Commander, Navy Network Warfare Command (COMNAVNETWARCOM), COMNAVNETWARCOM Information Operation Directorate.

(2) Only authorized personnel assigned to Fleet Information Warfare Center (FIWC), Radio NNWC Battalions, or other commands authorized by (acting as the Navy designated service cryptologic element), will conduct COMSEC Monitoring. COMNAVNETWARCOM will 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).

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

(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 contents of any telecommunications when such monitoring would constitute electronic surveillance.

(5) The results of COMSEC monitoring shall not be used to produce foreign intelligence or counterintelligence.

(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.

(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 5520.3B. 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.

6. 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 AIS equipment.

7. Authorization and Request

a. 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;

(2) When it will aid in protecting national security as described in paragraph 4; and

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

b. This instruction combines with periodic notices and reminders (issued by 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.

c. Commanding officers may request own force COMSEC monitoring through their chain of command.

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

9. 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 Department of Defense (DOD) telecommunications systems and AIS 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. The FLTCDRS will approve COMSEC monitoring requests and direct COMSEC monitoring operations for commands under their operational or administrative control.

c. COMNAVNETWARCOM will:

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

(2) Provide CNO advice and assistance on the conduct of COMSEC monitoring activities and procurement of COMSEC monitoring equipment.

(3) Conduct liaison with the NSA to ensure Navy compliance with national COMSEC monitoring directives.

(4) Ensure adequate numbers of personnel are properly trained for the conduct of COMSEC monitoring activities in the Navy.

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

d. The General Counsel of the Navy, in coordination with Judge Advocate General, will review the notification given to users of official DOD telecommunications systems and AIS within the Navy that such systems are subject to COMSEC monitoring and that use of such systems constitutes consent to COMSEC monitoring. The General Counsel shall state in writing for record purposes, on a biennial basis, a determination of the adequacy or inadequacy of such notification. If such notification is determined to be inadequate, the General Counsel of the Navy shall specify those measures necessary to make notification adequate.

10. Form. DD 2056 (12/85), Telephone Monitoring Notification Decal, S/N 0102-LF-002-0560, is available on Navy Forms OnLine https://forms.daps.dla.mil/

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.

COMSEC MONITORING TERMS AND DEFINITIONS

1. AIS (Automated Information 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 measures 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 AIS 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 AIS 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 AIS by other that local system administrators to include, but not limited to on-line surveys (OLS), Red Team operations, and naval computer incident response team (NAVCIRT) 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. Nonpublic Communications. A communication in which the parties thereto have a reasonable expectation of privacy.

6. Telecommunications. The transmission, communication, or processing of information, including the preparation of such information by electrical, electromagnetic, electromechanical, or electro-optical means.

7. 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.

8. TELMON (Telephone Monitoring). That portion of COMSEC monitoring which deals specifically with telephones.

PROCEDURES FOR COMSEC MONITORING OF TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

1. Request

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

b. Navy Echelon 2 commanders or commanders outside FLTCDR chain of command may submit request for conduct of COMSEC Monitoring of own or their subordinate's Department of the Navy (DON) telecommunications systems and AIS 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 AIS shall be notified that discussion/transmission of classified information over non-secure circuits is prohibited; that official DOD telecommunications systems and AIS are subject to COMSEC monitoring at all times; and that use of such telecommunications systems and AIS 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 deals (DD 2056) attached to the lower front portion.

d. All official Navy telephone directories will have this information prominently displayed on their covers in the following format:

"DO NOT DISCUSS CLASSIFIED INFORMATION ON NON-SECURE TELEPHONE. OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING FOR COMMUNICATIONS SECURITY PURPOSES AT ALL TIMES." 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 automated information systems (AIS) are required to display the following legally approved logon warning banner, which also serves to provided notification of, an consent to, COMSEC monitoring:

"THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY.

MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMIAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."