OPNAV INSTRUCTION 2201.3C

From: Chief of Naval Operations

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

Ref: (a) NTISSD No 600, National Telecommunications and Information System Security (NTISS) Communications Security (COMSEC) Monitoring, 10 April 1990 (NOTAL)
(b) DoD Instruction 8523.01 of 22 April 2008
(c) DoD Instruction 8560.01 of 22 August 2008

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

1. Purpose

a. To establish policy, procedures, and responsibilities governing communications security (COMSEC) monitoring within the Navy in compliance with references (a) through (c).

b. The 2000 series instructions apply to telecommunications and digital systems support. Changes to this instruction include updates to Navy organizational responsibilities and governance to align with current guidance.

2. Cancellation. OPNAVINST 2201.3B

3. Scope and Applicability. The provisions of this instruction are applicable to the U.S. Navy, including Government civilians, members of the active and reserve units, all contractors assigned to Navy activities, and all personnel who conduct contracted service for the Navy (e.g., research, development, test and evaluation agencies and their contracted agents).

4. Background

a. COMSEC monitoring is the act of listening to, copying, or recording transmissions of official telecommunications on organizational communications equipment in order to analyze the degree of security. 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 communications equipment, telephone, and information technology (IT) systems equipment.
b. This instruction does not pertain to:

   (1) systems administration and management functions to ensure proper installation, integration, and functionality of equipment and systems, including local security devices and systems;

   (2) signals intelligence, foreign intelligence, and counterintelligence collection activities; or

   (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 foreign intelligence threat. Such activities must be conducted in strict compliance with applicable laws, executive orders, applicable Presidential directives, and per references (a) through (c). Only authorized personnel assigned to Navy Cyber Defense Operations Command; Commanding Officer, Naval Network Warfare Command (COMNAVNETWARCOM), or other commands authorized by Commander, Fleet Cyber Command/TENTH Fleet, the Navy’s designated service cryptologic component, will conduct activities such as either red team or blue team operations, or both, including other activities that would constitute COMSEC monitoring under the auspices of the current definition.

   b. 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, when requested, per reference (a). When COMSEC monitoring is requested by a non-Navy entity for which Navy is the executive agent (e.g., U.S. Pacific Command), monitoring services are provided to the non-Navy entity through the joint COMSEC monitoring activity.

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

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

      (2) users of Government telecommunications 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 must not monitor, for COMSEC purposes, the content of any telecommunications when such monitoring would constitute electronic surveillance;

(5) per reference (c) the results of COMSEC monitoring will not be used to produce foreign intelligence or counter intelligence;

(6) no one within the Navy 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.

d. Following 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 crime, as defined under the Uniform Code of Military Justice, or similarly framed Federal, State, local, or foreign statutes, will be referred to the military commander or law enforcement agency having appropriate jurisdiction. 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.

e. COMSEC monitoring must 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 (OPNAV N09J) has lapsed and an emergent need to conduct COMSEC monitoring is identified, an echelon 2 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; and

(3) when the period of monitoring is for one year or less.
f. This instruction, combined with periodic notices and reminders (issued by an ALNAV message) serves as notification of Navy intent to monitor official communications of Navy commands and staff. Notification of specific COMSEC monitoring operations is not required.

g. Navy COMSEC monitoring activities must 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. **Deputy Chief of Naval Operations for Information Warfare (CNO N2N6) 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; and

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

b. **Fleet Maritime Operations Centers and Naval Component Commanders 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 fleet Maritime Operations Centers or Naval Component Commanders will request COMSEC monitoring operations from COMNAVNETWARCOM; and

   (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 the 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 fleet Maritime Operations Centers or Naval Component Commanders will notify their echelon 2 commander of the same compliance, and those echelon 2 commanders will provide notice to COMNAVNETWARCOM by 1 July of even-numbered years.

c. **COMNAVNETWARCOM will:**

   (1) approve specific COMSEC monitoring operations outside a fleet Maritime Operation Centers or Naval Component Commanders operational chain;
(2) compile the information supplied per 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 joint COMSEC monitoring activity 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 that conduct COMSEC monitoring; and

(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. 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 communications equipment, and IT systems equipment.

8. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy Directorate for Administration, Logistics, and Operations, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager or the Department of the Navy Directorate for Administration, Logistics, and Operations, Directives and Records Management Division program office.
9. **Review and Effective Date.** Per OPNAVINST 5215.17A, OPNAV N2N6F3 will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

MATTHEW. J. KOHLER  
Deputy Chief of Naval Operations  
for Information Warfare

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site [http://www.secnav.navy.mil/doni](http://www.secnav.navy.mil/doni)
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. Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons any information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Source: JP 6-0.

3. COMSEC Monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications in order to analyze the degree of security. 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. Any transmission, emission, or reception of: signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. Source: JP 6-0.

6. Telecommunications Systems. The interconnected devices used to either transmit or receive, or both, communications or to 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 Government equipment patched through the Naval Computer and Telecommunications Area Master Station, or Naval Computer and Telecommunications Station.
PROCEDURES FOR COMSEC MONITORING OF 
TELECOMMUNICATIONS AND IT SYSTEMS

1. Request

   a. Individual commands or commanders may submit requests for the conduct of COMSEC 
      monitoring of Navy telecommunications and IT systems via their operational chain of command 
      to the appropriate fleet Maritime Operation Centers or Naval Component Commanders.

   b. Navy echelon 2 commanders or commanders outside fleet Maritime Operation Centers or 
      Naval Component Commanders chain of command may submit requests for COMSEC 
      monitoring of their own or subordinates’ Department of the Navy Telecommunications and IT 
      systems to COMNAVNETWARCOM.

2. Notification. Commanding officers and unit commanders are responsible for ensuring that 
   notification, as identified in subparagraphs 2a through 2d, 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 must be notified that 
      discussion and 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, fact of consent to monitoring 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; communications-electronics 
      operating instructions; or similar documents.

   c. DoD telephones are provided for the transmissions of official Government information 
      and are subject to COMSEC monitoring at all times. Use of official DoD telephones constitutes 
      consent to COMSEC telephone monitoring, per reference (a).

   d. 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 the 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.