CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 211757Z APR 26 MID180038725536U
FM CNO WASHINGTON DC
TO NAVADMIN
INFO CNO WASHINGTON DC
BT
UNCLAS

NAVADMIN 093/26

MSGID/NAVADMIN/CNO WASHINGTON DC/N2N6/APR//

SUBJ/2026 COMMUNICATIONS SECURITY (COMSEC) MONITORING NOTIFICATION//

REF/A/INST/OPNAV/22MAY2020//
REF/B/INST/SECNAV/9MAY2019//
REF/C/INST/OPNAV/4APR2012//

NARR/REF A IS OPNAVINST 2201.3C - NAVY COMMUNICATIONS SECURITY MONITORING OF NAVY TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY SYSTEMS.
REF B IS SECNAVINST 3070.2A - DEPARTMENT OF THE NAVY OPERATIONS SECURITY INSTRUCTION.
REF C IS OPNAVINST 5450.345 - MISSION, FUNCTIONS AND TASKS INSTRUCTION FOR U.S. FLEET CYBER COMMAND.

RMKS/1. Communications Security (COMSEC) monitoring in the Navy is necessary in order to determine the degree of security provided to telecommunications and information technology (IT) systems; aid in countering their vulnerability to interception, technical exploitation, human intelligence threats, and other dimensions of foreign intelligence threats; and assess effectiveness of Operations Security (OPSEC) measures. Reference (a) implements policy that all Navy information systems and telecommunications systems, including government issued cellular devices, are subject to monitoring. This instruction can be obtained from the Department of the Navy (DON) issuance webpage at https://www.secnav.navy.mil/doni/opnav.aspx and should receive widest dissemination. All hands must understand the importance of practicing OPSEC and protecting critical unclassified information (reference (b)) while operating on Navy communication networks and devices.

2. Key elements of reference (a):
    a. Commanding Officers and Unit Commanders are responsible for ensuring that their crews and subordinates are regularly notified that official Department of War (DoW) telecommunications and IT systems are subject to COMSEC monitoring at all times.
    b. Consent to monitoring must be included in orientation briefings, daily bulletins or plans of the day/week, periodic training programs, and communications-electronic operating instructions or similar documents.
    c. DoW telephones and IT systems are provided for the transmission of official government information and are automatically subject to COMSEC monitoring at all times and must be appropriately labeled in accordance with enclosure (1) of reference (a). Use of DoW telephones constitutes consent to COMSEC monitoring. Discussion and transmission of classified information over non-secure circuits is prohibited.
    d. The standard consent banner, displayed upon logon to DoW IT systems, and user systems agreements (DON - User Agreement and Standard Mandatory

Notice and Consent Provision that must be signed alongside the DD2875) also serve to provide notification of, and consent to, COMSEC monitoring.

3. The biannual reporting criteria outlined in reference (a) remains unchanged. Fleet maritime operations centers, Naval component commanders, and Echelon 2 commanders are directed to verify implementation of the requirements outlined and provide notice to U.S. Fleet Cyber Command (FLTCYBERCOM) by 1 July 2026 confirming that subordinate commands are in compliance with the requirement to notify users of DoW telecommunications and IT systems that such systems are subject to COMSEC monitoring.

4. OPSEC note: OPSEC and COMSEC are mutually supportive, providing a measure of effectiveness of OPSEC measures. While it is necessary to share, discuss, email or post information while using official Navy networks and platforms, the Navy also has a responsibility to protect our critical information. Our adversaries are experts in aggregating pieces of unclassified information, often exploiting our mistakes or inadvertent disclosures of critical information from our open and unclassified networks. Proper application of OPSEC will help protect critical information while maintaining essential secrecy. By virtue of being a military professional, it is all our responsibility to use the utmost care and caution to protect the interests of our nation and keep our teammates safe. Think about this every time you use open systems or networks.

5. Released by Ms. Jennifer Edgin, Acting Deputy Chief of Naval Operations For Information Warfare, OPNAV N2N6.//

BT
#0001
NNNN
CLASSIFICATION: UNCLASSIFIED/