CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 181713Z FEB 25 MID180001628769U
FM CNO WASHINGTON DC
TO NAVADMIN
INFO CNO WASHINGTON DC
BT
UNCLAS

NAVADMIN 030/25

MSGID/NAVADMIN/CNO WASHINGTON DC/N2N6/FEB// CORRECTED COPY

SUBJ/NAVY OPERATIONS SECURITY (OPSEC)//

REF/A/INST/SECNAVINST 3070.2A/09MAY2019//
REF/B/INST/SECNAVINST 5720.44C CH-2/10APR2019//
REF/C/DOC/NTTP 3-13.3/DEC2022//
REF/D/-/NAVAL OPSEC SUPPORT TEAM/WEB//

NARR/REF A IS SECNAV OPSEC POLICY.
REF B IS SECNAV PUBLIC AFFAIRS POLICY.
REF C IS NAVY TACTICS, TECHNIQUES, AND PROCEDURES (OPSEC).
REF D IS THE NAVAL OPSEC SUPPORT TEAM WEBSITE AT:
https://www.navifor.usff.navy.mil/opsec/

POC/THERESA ADAIR/CDR/OPNAV OPSEC PM/ TEL: 703-695-8508/EMAIL:
THERESA.A.ADAIR.MIL@US.NAVY.MIL/ POC/NAVAL OPSEC SUPPORT TEAM/-/NAVIFOR
SUFFOLK/LOC: SUFFOLK VA/TEL: 757-203-3656/EMAIL: NAVY_OPSEC@US.NAVY.MIL//

RMKS/1. This message reiterates the guidance in references (a) through (d) and reminds all Navy personnel of Operations Security (OPSEC) best practices and the requirement for pre-publication release review.

2. Today our Navy is operating in the most complex, challenging, and contested information environment in history. Adversaries seek to gain and exploit vital Navy information through open source means such as social media posts, websites, publications, and public facing events. They identify, aggregate, and analyze multiple streams of unclassified information regarding Navy presence, capabilities, intent, readiness, timing and location of our operations, research and development programs, infrastructure, and networks.
An integral safeguard for unclassified but critical Navy information is proper use of OPSEC.

3. OPSEC is every Sailor's responsibility, from E-1 to O-10. OPSEC is more than an annual training requirement. It is common sense application of thoughtful and deliberate actions on a daily basis to minimize exposure of Navy information to actors who aim to undermine Navy's warfighting advantages. As a rule, you should assume that adversaries will view anything not hidden and read anything not secured or encrypted.

4. Social media platforms are important means to broaden public knowledge of America's warfighting Navy. They also present a great challenge to proper OPSEC. Avoid posting sensitive Navy information related to the categories in paragraph 2 and ask your family members to do the same. To update an old expression: "Loose tweets sink fleets."

5. While open discussion is necessary for any professional organization, special considerations must be made to limit an adversary's ability to gain and exploit insights into our vulnerabilities, weaknesses, and shortcomings.
Pre-publication review is a critical (and mandated) measure that ensures Navy professionals do not inadvertently disclose sensitive information in opinion pieces or scholarly articles.

6. Accordingly, all hands must submit any products for publication to their command OPSEC officer or Public Affairs Officer (PAO) for review prior to release into the public domain. Commands should seek outside review from appropriate subject matter experts or authorities if the topic is not within their mission area. For assistance, reach out to the OPNAV OPSEC Program Manager listed at the top of this message, and use the following websites: Defense office of prepublication and security review website (https://www.esd.whs.mil/dopsr/) and the Naval OPSEC Support Team website, reference (d).

7. Public facing events like air shows, fleet weeks, Navy community symposiums, and industry days are important forums to engage with the American public and Navy stakeholders. As with social media and publications, applying common-sense OPSEC measures during public facing events makes Navy information a harder target and safeguards Navy technology, operations, and people.

8. Released by VADM Karl O. Thomas, Deputy Chief of Naval Operations for Information Warfare, OPNAV N2N6.//

BT
#0001
NNNN
CLASSIFICATION: UNCLASSIFIED/