CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 061548Z OCT 25 MID320018356121U
FM CNO WASHINGTON DC
TO NAVADMIN
INFO CNO WASHINGTON DC
BT
UNCLAS

NAVADMIN 214/25

MSGID/GENADMIN/CNO WASHINGTON DC//N2N6/OCT/2025//

SUBJ/CYBERSECURITY AWARENESS MONTH 2025: FORTIFY AND DEFEND LETHALITY//

REF/A/DOC/DOD INSTRUCTION 8500.01/20140314//
REF/B/DOC/OPNAVINST 2201.2C/20180914//
REF/C/MEMO/CNO WASHINGTON DC/20230427//

NARR/REF A IS DOD INSTRUCTION 8500.01, CYBERSECURITY.
REF B IS OPNAVINST 2201.2C, UNITED STATES NAVY CYBERSECURITY PROGRAM.
REF C IS THE CHIEF OF NAVAL OPERATIONS MEMORANDUM ON PRIORITIZING
CYBERSECURITY.//

RMKS/1.This NAVADMIN announces October 2025 as Cybersecurity Awareness Month
(CSAM) and emphasizes the U.S. Navy's commitment to strengthening our cyber
defenses. This year's theme is "Fortify and Defend Lethality."

2. The cyber domain is a critical battlespace. Our ability to project
power, maintain readiness and achieve operational superiority depends on a
secure and resilient cyber environment. Our collective effort is essential
to maintaining a decisive advantage against adversaries.

3. "Fortify and Defend Lethality" highlights the direct correlation between
cybersecurity and our warfighting capabilities. A compromised system can
impair our weaponry, disrupt communications and expose critical information,
ultimately affecting our lethality.

4. Key focus areas for CSAM 2025 include:
    a. Threat awareness: stay informed about emerging cyber threats and
tactics used by adversaries. Understand the potential impact of compromised
systems on our operational capabilities. Report suspicious activity
immediately.
    b. Practice good cyber hygiene: regularly update passwords; enable
Multi-Factor Authentication (MFA); and be vigilant against phishing attempts.
Adhere to security protocols for all devices and systems. References (a) and
(b) provide detailed guidance on cybersecurity best practices.
    c. Secure remote work: follow established guidelines for secure remote
access, including using Government-Issued Devices, Encrypted Connections
(VPNs) and maintaining a secure home network. Be mindful of surroundings
when discussing sensitive information.
    d. Protect classified information: strictly adhere to data transfer
policies and report any potential data spillage immediately.
    e. Cybersecurity awareness: actively participate in cybersecurity
awareness opportunities for additional education to enhance your cyber skills
and knowledge.

5. Commands are encouraged to plan and execute CSAM activities throughout October, including:
    a. Cybersecurity awareness events.
    b.Posters and educational materials that display key cybersecurity messages.
    6.All hands are reminded that cybersecurity is everyone's responsibility. Our collective vigilance is the first line of defense. We must continuously strive to improve our cyber posture and maintain a strong defense against cyber threats.

7. Commands are encouraged to disseminate this message widely throughout their chain of command.

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

BT
#0001
NNNN
CLASSIFICATION: UNCLASSIFIED/