CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 151313Z APR 26 MID320018646872U
FM CNO WASHINGTON DC
TO NAVADMIN
INFO CNO WASHINGTON DC
BT
UNCLAS

NAVADMIN 084/26

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

SUBJ/ FISCAL YEAR 2026 CYBERSECURITY AWARENESS CHALLENGE//

REF/A/MSG/CNO WASHINGTON DC/ 151859Z OCT 24//
REF/B/DOC/SECNAVINST 5239.25/10 OCT 23//
REF/C/MSG/CNO WASHINGTON DC/231906Z MAR 26//

NARR/REF A IS NAVADMIN 214/24 PROVIDES GUIDANCE FOR THE FISCAL YEAR 2025 (FY25) CYBERSECURITY AWARENESS TRAINING.
REF B IS THE SECRETARY OF THE NAVY INSTRUCTION DEPARTMENT OF THE NAVY (DON) CYBERSPACE WORKFORCE QUALIFICATION AND MANAGEMENT PROGRAM.
REF C IS NAVADMIN 066/26, FISCAL YEAR 2026 COMMON MILITARY TRAINING REQUIREMENTS//

POC/LCDR BENJAMIN PITZEL/MIL/OPNAV N2N6D4/TEL: (571) 256-8291/E-MAIL: BENJAMIN.F.PITZEL.MIL(AT)US.NAVY.MIL//

RMKS/1. This NAVADMIN supersedes reference (a) and provides guidance for the Fiscal Year 2026 Cybersecurity Awareness Challenge (CAC) training requirement.

2. Per references (b) and (c), Navy personnel, civilians, and contractors with access to unclassified or classified networks must complete the Department of War (DoW) employee version of CAC by 1 September 2026.

3. Personnel who completed CAC 2025 after 30 September 2025 but before CAC 2026 is available shall receive credit for their annual FY26 training.

4. Total Workforce Management Services (TWMS) is the readiness platform used to track CAC completion percentages for the Navy. Commands and training platforms must confirm TWMS is capturing all CAC completions under the overarching requirement ID set by CNIC/TWMS Administration, eas(AT)ctirms.com, (TWMS Requirement ID: 77136- FY26 DoD Cyber Awareness Challenge) to receive credit. Commands are prohibited from creating additional CAC training requirements to set command specific training metrics. This requirement cannot be waived. The options below are the authorized methods for training delivery:
a.Commands can elect to complete CAC training using instructor-led delivery. A command designated cyber security professional such as the Information Systems Security Manager (ISSM) or Cyber Workforce Program Manager (CWF-PM) must provide the instruction.
b.Total Workforce Management Service (TWMS), https://twms.dc3n.navy.mil/;
c.Navy e-Learning (NEL), https://learning.nel.navy.mil/;

(Note: The My Navy Portal, https://learning.nel.navy.mil/ELIAASv2p/ev2Login.xhtml (redirects users to the NEL link)); d.Defense Information Systems Agency (DISA) website, https://www.cyber.mil/cyber-awareness-challenge;

e. Joint Knowledge Online (JKO), https://jkodirect.jten.mil/;

f. Waypoints, https://don.csod.com;

g. Other approved training sources, DISA Digital Video Discs (DVDs).

5. Ships can access the annual training from the NEL application hosted on the Navy Information/Application Product Suite (NIAPS) server, eliminating the need to reach back to shore hosted NEL websites. The CAC 2026 course is available via the NEL Afloat Learning Management System Pub Amendment 112 for download by the NIAPS Administrator using the normal manual NIAPS distance support update process. If unable to download Learning Management System Pub Amendment 112, ships can request a DVD with these files to be mailed by submitting a support request to Navy 311.

6. Although CAC training is an individual responsibility, commanders and commanding officers are accountable for 100 percent completion of their personnel. Effective September 1, 2020, the DoW Cybersecurity Hardening Scorecard collects information on the number of users who completed annual Cybersecurity Awareness training and the scorecard is briefed on a quarterly basis to the Deputy Secretary of War. Training officers are responsible for ensuring their personnel complete and properly document the required training.

7. Command training officers must validate training via TWMS or Fleet Training Management and Planning System (FLTMPS) (https://ntmpsweb.ncdc.navy.mil/fltmps/) authoritative databases. Training officers will manually record training completed via the DISA website, DISA DVDs, or instructor led. Manually record training in FLTMPS using the Learning Event Completion Form. Report any discrepancies to the Navy Training Management Planning System Operational Support office at ntmps.support(AT)navy.mil or 1-866-438-2898/DSN 922-1867.

8. The Command ISSM is responsible for reporting compliance to meet Federal Information Security Modernization Act of 2014 requirements. Command ISSMs will disable accounts of users who do not complete training by 1 September 2026 and maintain non-compliance list of accounts that were disabled.

9. This NAVADMIN will remain in effect until cancelled or superseded.

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

BT
#0001
NNNN
CLASSIFICATION: UNCLASSIFIED/