

CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 311838Z AUG 26 MID120041489897U
FM CNO WASHINGTON DC
TO NAVADMIN
INFO CNO WASHINGTON DC
BT
UNCLAS

NAVADMIN 204/26

MSGID/GENADMIN/CNO WASHINGTON DC/N6/N9/XXX//

Subj/MODIFICATION TO NAVADMIN 084/26 - FISCAL YEAR 2026 CYBERSECURITY
AWARENESS CHALLENGE TRAINING REQUIREMENTS //

REF/A/MSG/CNO WASHINGTON DC/151313Z APR 26//
REF/B/DOC/DOW CISO/14 APR 26//
REF/C/MEMO/SECWAR/15SEP25//

NARR/REF A IS NAVADMIN 084/26, FISCAL YEAR 2026 CYBERSECURITY AWARENESS
CHALLENGE POLICY
REF B IS THE DEPARTMENT OF WAR CHIEF INFORMATION SECURITY OFFICER MEMORANDUM,
REDUCTION OF ANNUAL CYBER AWARENESS TRAINING REQUIREMENTS
REF C IS THE SECRETARY OF WAR MEMORANDUM, REDUCTION OF MANDATORY TRAINING
REQUIREMENTS TO RESTORE MISSION FOCUS

POC/LCDR BENJAMIN PITZEL/MIL/OPNAV N99C/TEL: (571) 256-8291/
E-MAIL: BENJAMIN.F.PITZEL.MIL(AT)US.NAVY.MIL//

RMKS/1. Purpose. This NAVADMIN modifies reference (a) to align Department of
the Navy cybersecurity training requirements with the updated guidance
provided in references (b) and (c).

2. Policy Update. Effective immediately, the periodicity for the Department
of War (DoW) Cybersecurity Awareness Challenge (CAC) training is officially
changed for all active duty and reserve military personnel.

a. Military personnel are now required to complete the CAC upon initial
granting of network access and every three (3) years thereafter.

b. This supersedes the annual fiscal year requirement previously directed
in paragraph 2 of reference (a).

3. Civilian and Contractor Personnel. The relaxed periodicity applies
strictly to military personnel per reference (c). Department of the Navy
civilian employees and contractors must continue to complete the CAC on an
annual basis to maintain compliance with the Federal Information Security
Modernization Act (FISMA).

4. Training Systems Configuration.

a. Fleet Training Management and Planning System (FLTMPS) and Total
Workforce Management Services (TWMS) are currently being updated to reflect
this three-year periodicity for military members.

b. Until system updates are complete, commands shall locally track and
document compliance for military personnel who have completed the training
within the preceding 36 months to ensure network access is not erroneously
suspended.

5. Network Access Restrictions. Echelon II Command Information Officers (CIOs) will ensure that automated network account disablement scripts account for this modified periodicity for military accounts.

6. Released by VADM M. S. Wosje Deputy Chief of Naval Operations for Warfighting Requirements and Capabilities, N6N9//.

BT

#0001

NNNN

CLASSIFICATION: UNCLASSIFIED/