CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 192112Z AUG 26 MID120041446561U
FM SECNAV WASHINGTON DC
TO ALNAV
INFO SECNAV WASHINGTON DC
CNO WASHINGTON DC
BT
UNCLAS

ALNAV 050/26

MSGID/GENADMIN/SECNAV WASHINGTON DC/-/AUG//

SUBJ/EPIC VIGILANCE: IMMEDIATE ACTIONS FOR FORCE PROTECTION AND PERSONAL SECURITY//

RMKS/1. Since the initiation of Operation EPIC FURY, the Department of the Navy's (DON) personnel, assets, and our families face an evolving threat landscape. U.S. military installations and personnel remain under increased vigilance due to recent uncrewed aircraft system (UAS) encounters, suspicious activities, cyber threats, and acts of violence.
In response to these emerging threats, Naval Criminal Investigative Service (NCIS) implemented EPIC VIGILANCE, a DON-wide force protection initiative to detect, deter, and mitigate threats to DON installations and personnel. In the current global security climate, adversaries and hostile actors are executing a coordinated, multi-domain campaign against the DON enterprise. Recent incidents across the globe demonstrate a clear growth in adversary tactics, techniques, and procedures. These are not isolated events; they are part of a deliberate effort to gather intelligence, test our defenses, disrupt our operations, and intimidate our force. Key threat vectors include, but are not limited to:
a. Direct threats and harassment targeting our personnel and their families via social media and other online platforms, often including doxing (publication of personal information).
b. UAS surveillance of our warships, flight lines, and critical infrastructure, demonstrates increasing capability and intent to evade detection.
c. Ground-level surveillance and suspicious activity near our installations and in our communities.
d. Attempted physical attacks and probes against access control points, indicating a willingness by adversaries to move from threatening words to direct action.
e. Coordinated harassment campaigns designed to test security responses and personnel endurance at widely dispersed locations.

2. Every Sailor, Marine, civilian, and family member is a critical component of continued vigilance. Vigilance includes the following actions:
a. Harden your personal and family security posture:
Immediately review all social media accounts (including those of family members) for publicly available personal information. Set profiles to private. Remove any information that could identify your connection to the DON or reveal patterns of life. Adversaries are actively mining this data.
b. Report suspicious activity: Don't rationalize suspicious activity. Trust your instincts, a seemingly minor observation may be a critical component to identify and mitigate threats. Force protection is everyone's responsibility.

c. Maintain situational awareness: Be attentive to observed changes and anomalies in your daily activities at work, at home, and while in your communities.

d. Review and understand the force protection requirements for your command and area. Geographic Combatant Commanders direct minimum requirements for their respective areas of responsibility. Commanders should ensure that theater force protection requirements are briefed and understood by all personnel.

3. Based on recent events, personnel should immediately report observations of:

a. Possible surveillance: Individuals lingering near or photographing/filming gates, perimeter fences, ships, aircraft, or housing areas. Pay particular attention to the use of telephoto lenses or attempts to conceal the activity or depart hurriedly once observed.

b. Uncrewed system activity: Any uncrewed system operating near a DON installation, pier, flight line, or areas frequented by DON personnel, regardless of size, especially at night, or in vicinity of sensitive military locations.

c. Suspicious questioning/elicitation: Anyone showing undue interest in Department of War (DoW)/DON, asking unusual questions about ship or personnel movements, deployment dates, leadership schedules, base operations, or aggressively seeking personal information such addresses, social media accounts, email address, and phone numbers.

d. Targeting of personnel: Any instance of being followed, photographed, or confronted off-installation, particularly while in uniform or near your residence.

e. Cyber activity: Receipt of threatening or suspicious emails or social media messages by Service Members or family members; discovery of imposter social media accounts of shipmates.

4. As the DON lead agency for Counterintelligence Investigations (CI), NCIS conducts the full range of CI and counterterrorism activities to identify and neutralize Foreign Intelligence Entity targeting and exploitation of DON personnel, facilities, operations, and other resources.
Additionally, NCIS maintains exclusive investigative jurisdiction within the DON for the investigation of actual, suspected, or alleged major criminal offenses defined under the Uniform Code of Military Justice or civilian law. NCIS works with federal, state, local, and international partners to hold adversaries accountable and fuse intelligence to protect the DON from all threats. NCIS encourages DON equities to remain vigilant by staying up to date with local, national, and DoW media and alerts, reviewing Department of State advisories, being aware of their surroundings at all times, maintaining awareness of potential threats in their local areas of responsibilities, tracking credible threat reporting, and assessing the possibility of lone actors who may view DON personnel as targets of opportunity. NCIS reminds DON equities that large concentrations of people present attractive targets and encourages DON personnel and families to maintain low profiles at large-scale events.
Utilize the following mechanisms to report threats and suspicious activity immediately:

a. For immediate, life-threatening situations, call 911 first.

b. For non-life-threatening situations, immediately contact base security/Provost Marshal's office or local law enforcement (off-installation).

5. For all other suspicious activity, contact NCIS or your installation/force protection office:

a. NCIS Tips: The NCIS Tips website allows users to submit information to NCIS from their personal computer, tablet, or smart device at the below web site. You may also download and use the "NCIS Tips" application on your smartphone for anonymous or attributed reporting. https://www.ncis.navy.mil/Resources/NCIS-Tips/.

b. NCIS 24/7 duty desk: Contact your local NCIS field office. Phone numbers are available via your chain of command and at https://www.ncis.navy.mil/about-ncis/locations/.

c. The NCIS Multiple Threat Alert Center (MTAC) watch provides 24/7 indications and warnings for a wide range of threats to Navy and Marine Corps personnel and equities globally. The MTAC Watch can be reached at the following phone numbers/email addresses:

(1) MTAC Watch: (571) 305-4777
(2) MTAC NIPRNet email: mtac@ncis.navy.mil
(3) MTAC SIPRNet email: mtac@ncis.navy.smil.mil
(4) MTAC JWICS email: mtac@ncis.ic.gov
(5) TS VOIP: 980-0716
(6) Law Enforcement Desk: (571) 305-4900
(7) NCIS Hotline: 1-877-579-3648

d. For Marine Corps Personnel, suspicious activity can be also reported via the USMC Eagle Eyes Website (https://usmceagleeyes.org/). Headquarters Marine Corps operates the Threat Fusion Cell, which is collocated within the NCIS MTAC and can be contacted at mtac_usmc_lnos@ncis.navy.mil or 571-305-4765.

6. Our greatest strength is our unity and our shared commitment to protect one another. By embracing this heightened posture of vigilance, we will safeguard our force, protect our families, and ensure the unhindered execution of our national security mission.

7. Released by the Honorable Hung Cao, Acting Secretary of the Navy.//

BT
#0001
NNNN
CLASSIFICATION: UNCLASSIFIED/