CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 271649Z FEB 25 MID180001636599U
FM SECNAV WASHINGTON DC
TO ALNAV
INFO CMC WASHINGTON DC
CNO WASHINGTON DC
SECNAV WASHINGTON DC
BT
UNCLAS

ALNAV 018/25

MSGID/GENADMIN/SECNAV WASHINGTON DC/-/FEB//

SUBJ/FOREIGN ADVERSARY TARGETING OF UNITED STATES NAVY AND MARINE CORPS PERSONNEL ON SOCIAL MEDIA//

REF/A/MSG/ALNAV/29AUG24//
REF/B/DOC/OPNAVINST/14JUN24//
REF/C/DOC/SECNAVINST/28OCT19//
REF/D//DOC/MCO/12NOV20//
REF/E/DOC/DODD/17MAY11//

NARR/REF A IS ALNAV 073/24, DEPARTMENT OF THE NAVY INSIDER THREAT AWARENESS MONTH.
REF B IS OPNAVINST 5510.165B, NAVY INSIDER THREAT PROGRAM.
REF C IS SECNAVINST 5510.37A, DEPARTMENT OF THE NAVY INSIDER THREAT PROGRAM.
REF D IS MARINE CORPS ORDER 5510.21, MARINE CORPS COUNTER-INSIDER THREAT PROGRAM.
REF E IS DOD DIRECTIVE 5240.06, COUNTERINTELLIGENCE AWARENESS AND REPORTING.

RMKS/1. Foreign Intelligence Entities (FIE) are using Social Networking Sites (SNS) and applications to target Department of Defense (DoD) and Department of the Navy (DON) personnel and their families to access facilities, systems, equipment, information, or infrastructure in order to damage, disrupt operations, compromise information or commit espionage on behalf of an adversary or competitor. FIE are also using fake personas to obfuscate their intent and affiliation with foreign intelligence services.
They have been observed as increasing their use of SNS and seemingly legitimate job offers to elicit sensitive information. These solicitations pose a direct threat to our defense industrial base and undermine the ability of our Department to compete with foreign competitors on the development of critical emerging technologies. The detection and deterrence of these efforts should be a priority for all active duty and civilian members of the DON. The Naval Criminal Investigative Service (NCIS) and the DON's Insider Threat Programs are committed to increasing the awareness of these threats pursuant to references (a) through (d).

2. Platforms and Tactics. FIE are leveraging SNS to insidiously obtain

unclassified and classified information from U.S. military and other U.S. Government (USG) entities and affiliates. FIE have used SNS such as Facebook, LinkedIn, and Indeed to initiate espionage relationships with DoD and other USG personnel by posing as researchers and headhunters and offering jobs and consulting opportunities. Contact requests are initiated with superficially harmless questions in order to establish rapport and determine military affiliation. FIE and those working on their behalf are known to offer all-expense paid trips to their targets for speaking engagements, such as presentations at universities and interviews.

3. Solicitation Questions. The questions asked may not explicitly or directly include classified information, rather, adversaries may rely on opinion-based queries to gather information. Examples include geopolitical questions on U.S. relations with China, Taiwan, or Ukraine; opinions on the current U.S. military command climate and structure; or opinions on how to improve military operations and/or functions. Adversaries may also offer disproportionately high payments for opinion papers on the aforementioned topics. Although this model of solicitation does not fit the traditional methods of targeting personnel with access to classified information, the threat should not be discounted, regardless of how innocuous the requested information appears.

4. Contact Methods. Methods of contact include, but are not limited to, social media direct messages, email, phishing attempts, or telephone calls. These contacts appear benign in nature and often do not seem to originate from a hostile nation or government, but rather appear to originate from within the United States or from a friendly nation. The requests have been known to escalate from the sharing of opinions to veiled requests for classified material. All DON personnel are encouraged to remain vigilant to this active and highly complex national security threat.

5. Financial Solicitations. Additionally, DON personnel and their families should be vigilant for suspected fraudulent financial solicitations. FIE use a combination of fake websites, phishing messages, and malicious apps to trick DON personnel into providing financial data, and/or login credentials used for long-term access to financial accounts which are then exploited for vulnerabilities.

6. Reporting Requirements. As mandated by reference (e), all DON personnel will report potential FIE threats, to include contacts, activities, indicators, and behaviors, to their organization's counterintelligence (CI) element or the NCIS. When CI support is not available, DON personnel shall report the threat without delay to their security officer, supervisor, or commander - who shall forward reported information to their organizational CI element or NCIS within 72 hours.

7. All commanding officers and supervisors should mandate prompt threat reporting in order to deter efforts by our adversaries to undermine our military and enhance awareness of established procedures for contacting their respective CI organization and the assigned NCIS Special Agent, servicing NCIS office, or Navy or Marine Corps Insider Threat program representative.

Reports can also be submitted to NCIS via the "SUBMIT A TIP" link at the top of the NCIS home page located at https://www.ncis.navy.mil/.

8. Released by Mr. Terence G. Emmert, Acting Secretary of the Navy.//

BT
#0001
NNNN
CLASSIFICATION: UNCLASSIFIED/