DEPARTMENT OF THE NAVY
UNITED STATES NAVAL ACADEMY
121 BLAKE ROAD
ANNAPOLIS MARYLAND 21402-1300

USNAINST 3432.1
PAO
23 MAR 2015

USNA INSTRUCTION 3432.1

From: Superintendent, United States Naval Academy

Subj: OPERATIONS SECURITY

Ref: (a) OPNAVINST 3432.1A
(b) SECNAVINST 5210.16

Encl: (1) U.S. Naval Academy OPSEC Program Management Responsibilities and Governance

1. Purpose. To establish policy, procedures and responsibilities for the U.S. Naval Academy (USNA) Operations Security (OPSEC) program.

2. Applicability. The provisions of this instruction are applicable to USNA personnel, all contractors assigned to USNA activities, and all personnel conducting contracted service for USNA.

3. Background. OPSEC is a critical process for all Navy activities. The practice of OPSEC enables mission success by preventing inadvertent compromise of sensitive or classified activities, capabilities, or intentions at the tactical, operational and strategic levels. OPSEC processes provide commanders with the ability to identify critical information (CI), current vulnerabilities, risks due to these vulnerabilities, and countermeasure decision criteria to mitigate risks.

4. Policy. USNA's goal is to establish and implement the best OPSEC policies, procedures, processes and guidance to enable sustained superior performance and cost effective protection of Navy CI, people, operations, and technology. USNA shall institute and manage an OPSEC program relevant to mission and resources per reference (a) and enclosure (1).

5. Records Management. Records created as a result of this instruction shall be managed per reference (b).

S. S. VAHSEN
Chief of Staff

Distribution:
All Non Mids (electronically)

U.S. NAVAL ACADEMY OPSEC PROGRAM MANAGEMENT RESPONSIBILITES AND GOVERNANCE

1. Assigned Personnel. All military, government civilian, and contractor personnel assigned to USNA units and activities are responsible for compliance with this governance.

2. Superintendent

a. Has overall responsibility for development of USNA's OPSEC policy.

b. Shall advise the Chief of Naval Operations concerning USNA OPSEC matters.

c. Shall appoint an OPSEC program manager in writing. The designee will have insight to the full scope of the command's mission and may manage the OPSEC program full-time or as a collateral duty.

3. OPSEC Program Manager. The USNA OPSEC Program Manager shall complete core competency OPSEC training and develop, manage, and execute USNA's OPSEC program. The OPSEC Program Manager is responsible for the following:

a. Coordinate and administer USNA's OPSEC program and execute command OPSEC instruction per references (a).

b. Once Secure Internet Protocol Router Network (SIPRNET) access is established, maintain an account with the Operations Security Collaboration Architecture (OSCAR) program. This program was developed as an interactive tool for conducting an OPSEC assessment and incorporates intelligence information with user-supplied settings that reflect the current command environment. Assessment results can provide a snapshot of the USNA's current OPSEC posture (e.g., susceptibility to open-source adversary intelligence collection). Use of OSCAR annually will satisfy the annual assessment requirements.

c. Determine command CI. CI that has been fully coordinated within an organization and approved by the senior decision maker will be visible and used by all personnel in the

organization to identify unclassified information requiring application of OPSEC measures.

d. Ensure classified and unclassified contract requirements properly reflect OPSEC responsibilities and that these responsibilities are included in contracts when applicable.

e. Complete an OPSEC assessment annually per reference (a).

f. Maintain a turnover binder and ensure OPSEC programs and plans are exercised or evaluated through regular assessments.

g. Generate and submit an annual OPSEC program status report to CNO's OPSEC program manager no later than 1 November each year.

h. Lead internal local OPSEC working group meetings. An internal OPSEC working group should consist of at least one representative entitled "OPSEC coordinator" from each directorate, department or division, especially the following representatives: Administrative, Comptroller, Naval Academy Business Services Division, Information Technology Services Division, Brigade Operations, Special Events and NSA Annapolis security.

i. Provide OPSEC orientation and awareness training to assigned personnel. Ensure OPSEC awareness training is conducted at least annually.

j. Maintain USNA's OPSEC instruction.

k. Provide oversight of Naval Academy Preparatory School OPSEC practices.

l. Review USNA's publicly available media and Web sites for the following concerns:

(1) Unclassified, publicly available Web sites shall not include classified material, "For Official Use Only" information, proprietary information, or information that could enable the recipient to infer this type of information. Personnel are reminded that all government information must be approved by USNA leadership for public release.

(2) Unclassified, publicly available Web sites shall not display personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers, or e-mail addresses which contain the individual's name. General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable. The names, telephone numbers, and personalized, official e-mail addresses of command or activity public affairs personnel and or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories. Guidelines for official Internet posts can be found in ALNAV 056/10.

(3) Public affairs is an important tool in garnering public support, fostering community relations, and helping with the attainment of USNA's mission. Public knowledge of military operations is inevitable because of advanced technology and instant media coverage. Therefore, publicly accessible information must be considered from an adversary's perspective prior to publication where media attention is expected or desired. The need for OPSEC should not be used as an excuse to deny non-CI to the public.

(4) The use of social media for Federal services and interactions is growing tremendously, supported by initiatives from the federal government and demands from the public. This situation presents both opportunity and risk. USNA personnel are encouraged to responsibly engage in the use of social media and social networking sites in an unofficial and personal capacity.

(5) Guidelines and recommendations for using social media technologies in a manner that minimizes the risk are located in ALNAV 056-057/10, U.S. Navy Chief of Information Social Media Web page (https://www.chinfo.navy.mil/socialmedia.html). If USNA personnel have any questions regarding the appropriateness of information they intend to place on social media sites, they should obtain guidance both from USNA's OPSEC Manager and Public Affairs Officer.