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

USNAINST 3432.1A
28/Pers Ofcr
19 Jul 2023

USNA INSTRUCTION 3432.1A

From: Superintendent, United States Naval Academy

Subj: OPERATIONS SECURITY

Ref: (a) OPNAVINST 3432.1A
(b) USNAINST 5720.3F
(c) SECNAVINST 5720.44C
(d) SECNAVINST 3070.2A
(e) Joint Pub 3-13.3 of 6 January 2016
(f) DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual with Change 2 of 29 October 2020
(g) CJCSI 3213.01D of 7 May 2012

Encl: (1) U.S. Naval Academy OPSEC Program Management Responsibilities and Governance
(2) U.S. Naval Academy Critical Information and Indicators List
(3) U.S. Naval Academy Operations Security Process

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

2. Cancellation. USNAINST 3432.1.

3. Scope. The provisions of this instruction are applicable to USNA assigned personnel as defined in enclosure (1).

4. 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.

5. 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 will institute and manage an OPSEC program relevant to mission and resources per reference (a) and enclosure (1).

6. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-InformationManagement/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local record custodian or the USNA Records Manager.

7. Review and Effective Date. The OPSEC program manager will review this instruction annually on the anniversary of the effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/9 Review of Instruction.

8. Information Controls. The annual reporting requirements described in Enclosure (1) paragraph 3.g. have been assigned Report Control Symbol (RCS) DDINTEL(A)2228 per DoDM 5205.02.

J. S. BATES
Chief of Staff

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the USNA Issuance Website, https://www.usna.edu/AdminSupport/Inst/

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

1. Assigned Personnel. All 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. Will advise the Chief of Naval Operations concerning USNA OPSEC matters.

c. Will 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 will 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 reference (a) and enclosure (3).

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 continuity of operations 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, including midshipmen. 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 will not include classified material, "Controlled Unclassified 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 per reference (b).

(2) Unclassified, publicly available websites will not display personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers, or email addresses which contain the individual's name. Exceptions per reference (c) are:

(a) General telephone numbers and non-personalized email addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable. The names, telephone numbers, and personalized, official email 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.

(b) The professional academic staff may be identified by name, specialty, etc., as required to maintain academic standing. Additionally, the faculty may interact with the public as part of the process of recruiting students, and thus some identifying information is appropriate. However, such information may include only professional information and not information on their families, place of birth, hobbies, etc., or other information not related to their academic credentials.

(c) The contact information for support staff and other departments will be generic and will not contain personal information, e.g., Admissions Office, phone XXX-XXX-XXXX, email: admissionsusna@usna.edu. Guidelines for official internet posts can be found in ALNAV 056/10.

(3) Public affairs are 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 056/10, ALNAV 057/10, and the Navy Social Media Handbook. 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.

U.S. NAVAL ACADEMY CRITICAL INFORMATION AND INDICATORS LIST

1. U.S. Naval Academy (USNA) Critical Information is information adversaries need to obtain in order to gain an advantage over or impose unacceptable consequences on U.S. military forces. Operations Security (OPSEC), unlike security of classified information, is an operational function aimed at protecting unclassified controlled or critical information. Seemingly harmless data combined with other conversations or documents could reveal sensitive or classified information, compromising U.S. and/or Allied capabilities or limitations.

2. Every individual assigned to USNA is responsible for protecting this critical information including faculty, staff, and students. USNA personnel have an explicit responsibility for understanding and protecting OPSEC concerns highlighted by Topic Sponsors or other partners that need to be protected from inadvertent or improper disclosure. The following Critical Information and Indicators List (CIIL) is a guide for the types of information to protect from public release or foreign national disclosure:

a. Details of research proposals, studies, journal articles, public conference presentations, experiments, tests, or other activities leading to development of, or identifying vulnerabilities in, sensitive defense capabilities.

b. Course content or syllabi for courses addressing capabilities in sensitive mission areas such as Directed Energy, Cyber, Intelligence, Advanced Materials, Energetics, and Machine Learning and Robotics.

c. Existence and/or details of intrusions into or attacks against Department of Defense networks or information systems, including the tactics, techniques and procedures used, vulnerabilities exploited, and data targeted for exploitation.

d. Association of abbreviations, acronyms, nicknames, or code words with sensitive projects or locations.

e. Reference of mission-associated information, such as personnel/equipment deployment dates or locations, personnel numbers, purpose, itineraries, duration, systems involved, and personally identifiable information. This is especially true if embedded with operational units, such as ships, submarines, squadrons, or teams.

f. Major degradation of USNA research capabilities (such as loss of key laboratory equipment or classified network access) or improved research advances.

g. Specifics concerning Distinguished Visitors to USNA, including foreign dignitaries or contingents of a sensitive nature, revealing details such as lodging, exact time of arrival/departure, and subject of meetings (outside of regular announcements).

h. Network and information systems user identifications and Passwords.

i. Critical Information and Critical Program Information obtained from Resource Sponsors in support of USNA research.

j. Specific operating systems and software running on USNA systems, to include software version numbers.

3. Per reference (d), the following information is generally not releasable unless declared otherwise by applicable public affairs guidance (Public Affairs Officer) or higher operational authority, or approved for public release:

a. Future plans or operations

b. Detailed information about vulnerabilities or weaknesses

c. Rules of engagement

d. Security measures, force protection, or deceptive actions used as part of an operation

e. Intelligence collection activities (past and present), including intelligence methods, targets and results

f. Specific types of ordnance expended, and (in some cases) the methods

g. Location and activities of special operations

h. Details of active law enforcement investigations

4. Primarily, OPSEC is a risk management process that considers the risks of disclosure in conjunction with the benefits of sharing information to build knowledge. It includes awareness of sensitive information and thinking about how something looks from an adversary's viewpoint. OPSEC is carried out through conscientious protection of key pieces of information, keeping them out of the view and preventing dissemination to unintended recipients through judicious filtering of public-facing material, use of Distribution Statements, review of conference materials, encrypted e-mail, secure telephones, etc.

5. This CIIL should be reviewed annually.

U.S. NAVAL ACADEMY OPERATIONS SECURITY PROCESS

1. General

a. Operation Security (OPSEC) planning is a five-step process explicated in reference (e), normally applied in sequential order. Individual steps may be revisited at any time, as required. New information about an adversary's capabilities or intentions, for instance, would require new analysis of threats. The OPSEC process should be conducted individually by those conducting research and education programs, such as Principal Investigators. The U.S. Naval Academy (USNA) OPSEC process is conducted organizationally by the OPSEC Working Group.

b. An understanding of the following terms is required before the process can be explained:

(1) Critical Information (CI). Specific facts about friendly intentions, capabilities, and activities for which adversaries need to plan and act effectively on to guarantee the failure of, or result in unacceptable consequences for, friendly mission accomplishment. In the context of USNA, this might be information about an ongoing engineering research analysis of U.S. Navy ship components that seeks to identify critical vulnerabilities.

(2) OPSEC indicators. Friendly, detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

(3) OPSEC vulnerability. A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

2. The 5-Step OPSEC Process

a. OPSEC Step 1 - Identification of Critical Information

(1) The USNA OPSEC Working Group will seek to identify unclassified, sensitive information and other sensitive activities at USNA whose intentions, capabilities, and activities can aid an adversary in developing a better understanding of Department of Defense (DoD) current and future technologies and operational strategies.

(2) USNA CI could be information that is vitally needed by an adversary. Critical information is important in that it focuses the OPSEC process on protecting vital information rather than attempting to protect all sensitive information. USNA's critical information can be found in enclosure (2) and will be made available to staff, faculty and students via their respective OPSEC Coordinators. Examples of critical information are provided in reference (a).

b. OPSEC Step 2 - Analysis of Threats

(1) This action involves the research and analysis of intelligence information, counterintelligence, reports, and open source information to identify who the likely adversaries are with respect to USNA research and the technology as it pertains to DoD.

(2) The OPSEC Working Group will seek answers to the following questions:

(a) Who is the adversary? (Who has the intent and capability to take action against the planned activity?)

(b) What are the adversary's goals? (What does the adversary want to accomplish?)

(c) What actions might the adversary take?

(d) What critical information does the adversary already know about the operation?

(e) What are the adversary's intelligence collection capabilities?

(f) Detailed information about the adversary's intelligence collection capabilities will be obtained from USNA supporting counterintelligence and intelligence organizations.

c. OPSEC Step 3 - Analysis of Vulnerability.

(1) This action identifies an operation's or activity's OPSEC vulnerabilities. It requires examining each aspect to identify any OPSEC indicators that could reveal critical information, and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it, and then taking timely action.

(2) Continuing to work with other security elements at USNA, USNA personnel must seek answers to the following questions:

(a) What indicators (friendly actions and open source information) of critical information not known to the adversary will be created by the friendly activities (to include making information about USNA research publicly available)?

(b) What indicators can the adversary actually collect?

(c) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?). Indicators might include:

1. Deployment schedules for sensitive programs.

2. Identity of units/personnel for sensitive operations.

3. Funding levels for sensitive operations.

4. Detailed inventory of test equipment.

5. Organizational charts and personnel rosters for sensitive programs.

6. High level military/civilian interest.

d. OPSEC Step 4 - Assessment of Risk

(1) There are two actions to this component. First, analyze the OPSEC vulnerabilities identified in the previous action, quantify the risk presented from each vulnerability in accordance with reference (f), and identify possible OPSEC measures for each vulnerability. Second, specific OPSEC measures are then selected for execution based upon a risk assessment completed by the superintendent and staff.

(2) OPSEC measures reduce the probability of the adversary either collecting the indicators or being able to correctly analyze their meaning.

(a) OPSEC measures can be used to:

1. Prevent the adversary from detecting an indicator.

2. Provide an alternative analysis of an indicator.

3. Attack the adversary's collection system.

(b) OPSEC measures include, among other actions, ensuring public information regarding USNA education and research is properly reviewed and disseminated in a way that will work against the adversary's intelligence collection efforts.

(c) More than one possible measure may be identified for each vulnerability. Conversely, a single measure may be used for more than one vulnerability. The most desirable OPSEC measures are those that combine the highest possible protection with the least impact on mission effectiveness.

(d) Appendix C of reference (g), provides OPSEC security measures; e.g., at USNA, these might include but are not limited to:

1. Controlled distribution of personal travel calendars/itineraries.

2. Protection of personally identifiable information (PII).

3. Critical communications and computer locations, support, techniques, limitations, effectiveness, and outages that support or impact USNA mission(s), including Internet Protocol address mapping, server configuration, firewall characteristics, and user identifications and passwords.

(4) Review of research reports for critical information prior to publication.

(3) The OPSEC Working Group will produce a risk assessment that requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

(a) OPSEC measures usually entail some cost in time, resources, personnel, or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires command involvement.

(b) Typical questions that might be asked when making this analysis include:

1. What risk to effectiveness is likely to occur if a particular OPSEC measure is implemented?

2. What risk to mission success (not just to USNA, but to the larger Navy and DoD mission of national defense) is likely to occur if an OPSEC measure is not implemented?

3. What risk to mission success is likely if an OPSEC measure fails to be effective?

(c) The interaction of OPSEC measures must be analyzed. In some situations, certain OPSEC measures may actually create indicators of critical information. For example: suddenly eliminating certain types of public correspondence or advertising about USNA and its research could alert foreign collection activities of a sensitive research area.

(4) The selection of measures must be coordinated outside the OPSEC Working Group. Decisions on OPSEC measures cannot be made in a vacuum. For example: USNA faculty and staff must seriously consider the OPSEC implications of information released to the public.

e. OPSEC Step 5 - Application of Appropriate OPSEC Measures. In this step, the command implements the OPSEC measures selected in OPSEC Step 4.