DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

IN REPLY REFER TO
NAVSEAINST 3070.2
Ser 00P/476
31 Dec 2021

NAVSEA INSTRUCTION 3070.2

From: Commander, Naval Sea Systems Command

Subj: NAVAL SEA SYSTEMS COMMAND OPERATIONS SECURITY

Ref: (a) DoD Directive 5205.02E, DoD Operations Security (OPSEC) Program of 20 June 2012
(b) SECNAVINST 3070.2A
(c) DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual of 3 November 2008
(d) OPNAVINST 3432.1A
(e) DoDM 5220.22, Volume 2, National Industrial Security Program: Industrial Security Procedures for Government Activities, of 1 August 2018
(f) DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release of 13 August 2014
(g) NAVSEAINST 5230.12A
(h) SECNAVINST 5720.44C
(i) DoDM 5105.21, Volume 2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control and Technical Security, of 19 October 2012
(j) NAVSEAINST 5527.1

1. Purpose

a. This instruction establishes policy, responsibilities, management structure, and guidance for implementing and managing the Naval Sea Systems Command (NAVSEA) Operations Security (OPSEC) program throughout the NAVSEA Enterprise, following the guidance, processes and recommendations set in references (a), (b), (c) and (d).

b. The Standard Subject Identification Code (SSIC) for this instruction was changed from '3432' to '3070', aligning with similar Department of the Navy (DON) redesignation of reference (b).

2. Cancellation: NAVSEAINST 3432.1A.

3. Significant changes, updates and/or additions:

a. Inclusion of procedures for security and content review of official information considered for release into the public domain.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

b. Research and review of publicly accessible and internet open sources for presence of NAVSEA Enterprise critical information and indicators (CII) and/or sensitive data.

c. Completion of OPSEC awareness training requirements prior to granting employee access to Department of the Navy (DON) information technology systems and networks.

d. Designation of appropriate command OPSEC program level.

e. Safeguarding and protection of designated command critical information.

f. OPSEC and Technical Surveillance Countermeasures (TSCM).

4. Applicability

a. NAVSEA's unique mission and overall strategy dictate that we strictly adhere to OPSEC policy and procedures in order to achieve operational superiority. As such, the provisions of this instruction apply to all NAVSEA Headquarters (HQ) and subordinate commands, collectively referred to as the 'NAVSEA Enterprise.' The NAVSEA Enterprise will fully implement DON OPSEC requirements to help safeguard NAVSEA critical information and help deny observation and collection of indicators by potential adversaries.

b. All military, civilian, and 'seated' contractor personnel, assigned to, or attached to the NAVSEA Enterprise are required to fully comply with this instruction. All OPSEC Program Managers (PM), OPSEC Officers and OPSEC Coordinators must become familiar with the OPSEC policy, guidance, and best practices delineated in references (a) through (d).

5. Background

a. OPSEC is a process of identifying, analyzing and controlling critical information indicating friendly actions associated with military operations and other activities, per references (a) through (d). Specific purposes of OPSEC are to:

(1) Identify those actions that can be observed by adversary intelligence systems;

(2) Determine what specific indications could be collected, analyzed and interpreted to derive critical information in time to be useful to adversaries; and

(3) Select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

b. The National OPSEC program, established by National Security Presidential Memorandum-28, is based on the recognition that, even though traditional security programs and procedures to protect classified matters exist, unclassified information and certain detectable operational activities can reveal the existence of, and sometimes details about, classified or sensitive activities. OPSEC ties together all the elements of a comprehensive security program and forms the basis for effective, overall security program management. OPSEC enhances and supplements traditional security programs.

c. A strong effective NAVSEA OPSEC program is necessary to protect NAVSEA CII from adversary collection activities. Routinely applying OPSEC in daily operations or during the planning phase of any event or operation, can greatly enhance NAVSEA's effectiveness in protecting relevant critical information from adversary collection and exploitation.

6. Responsibilities

a. Commander, Naval Sea Systems Command (SEA 00), or their designate, will:

(1) Establish, resource, and maintain an effective HQ NAVSEA OPSEC program;

(2) Ensure the HQ NAVSEA OPSEC program is designated as a Level-III program per references (b) and (c);

(3) Approve and issue a NAVSEA Enterprise OPSEC policy instruction or applicable guidance;

(4) Approve the HQ NAVSEA critical information and indicators list (CIIL) and ensure the CIIL is reviewed annually per references (b) and (c);

(5) As tasked and when directed, biennially report the status of the NAVSEA Enterprise OPSEC program to the Deputy Under Secretary of Defense for Intelligence and Security (OUSD (I&S)), via the Office of the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6), per references (a) through (d).

b. Within NAVSEA HQ, the NAVSEA OPSEC program functions reside in the Office of Security Programs under the direction of the NAVSEA Director of Security Programs/Activity Security Manager (ASM) (SEA 00P). This office will:

(1) Monitor and oversee OPSEC policy and activities for, and within the NAVSEA Enterprise, as well as provide management oversight to subordinate echelon 3 and 4 commands;

(2) Facilitate coordination of OPSEC matters within the NAVSEA Enterprise through the NAVSEA Security Community of Practice or directly to individual NAVSEA Enterprise components, as applicable; and

(3) Task NAVSEA Enterprise Security Directors/Activity Security Managers, as required, to ensure compliance with all applicable OPSEC policy requirements and other security related taskings.

c. The NAVSEA HQ OPSEC PM will:

(1) Be responsible for administering the OPSEC Program at NAVSEA HQ and providing oversight of OPSEC programs throughout the NAVSEA Enterprise per references (a) through (d), and as directed by NAVSEA SEA 00P;

(2) Provide guidance, oversight and assessments of echelon 3- and 4-level OPSEC programs throughout the NAVSEA Enterprise;

(3) When directed, compile the consolidated NAVSEA-wide input to the biennial (OUSD (I&S)), OPSEC status report;

(4) Augment the NAVSEA HQ Inspector General (SEA 00N), as required, to validate compliance of echelon 3- and 4-level OPSEC programs throughout the NAVSEA Enterprise;

d. OPSEC PMs, OPSEC Coordinators and/or OPSEC Officers at all NAVSEA echelons, responsible for program oversight, will:

(1) Be appointed in writing;

(2) Coordinate with command leadership to ensure command OPSEC programs are designated at the appropriate level, per enclosure 3 of reference (c). Appropriate program designation level can be based upon, or affected by, such things as overall Security element manning levels, experience of OPSEC PM/Coordinator; additional duties of OPSEC PM/Coordinator, command organizational structure, budgetary resources, etc. (listing of examples not all inclusive).

(3) Act as the Commander's subject matter expert (SME) on all matters pertaining to OPSEC;

(4) Complete applicable OPSEC education and training. Specifically, per enclosure 7 of reference (c), all personnel assigned to OPSEC-related duties must satisfy both preparatory and sustaining Department of Defense (DoD) standard education and training requirements upon assignment.

(5) Conduct annual OPSEC program assessments/self-inspections, maintain file copies of applicable reports and provide info copies to higher headquarters elements;

(6) Per references (a) and (c), conduct OPSEC oversight assessments of subordinate command programs using the published OPSEC guidance to determine if the unit being assessed

is correctly implementing higher headquarters (HHQ) directed, and their local, OPSEC policies and procedures;

(7) Assist Commanders, Commanding Officers, PMs, and supervisors with integrating OPSEC into all applicable command activities;

(8) Implement and promote an effective OPSEC training, education and awareness campaign among command personnel, which includes overview of the OPSEC process, command critical information, adversary intelligence threats (in concert with the Navy Criminal Investigative Service (NCIS)), controlled unclassified information (CUI), public release review, social media, geotagging concerns and individual employee OPSEC responsibilities, per references (a), (b) and (c);

(9) Conduct and oversee initial OPSEC awareness training in conjunction with unit onboarding indoctrination. Ensure annual OPSEC refresher training is provided for all military, civilian, and seated contractor personnel per references (b) and (c).

(10) Verify and validate classified and unclassified contracts properly reflect OPSEC requirements and responsibilities, when applicable, through formal review of Statement of Work (SOW), Request for Proposal (RFP) or Performance Work Statement (PWS) type products;

(11) Compile command OPSEC policy guidance for approval and signature by command leadership, as applicable;

(12) Chair the NAVSEA OPSEC Working Group (OWG);

(13) Compile command CIIL, with assistance of the OWG, for leadership approval, in addition, annually review the CIIL and update, as applicable, per references (a) through (d), also ensure CIIL is made accessible to all command personnel;

(14) As necessary, coordinate with NCIS for counterintelligence and threat support to mitigate potential OPSEC vulnerabilities and develop effective countermeasures;

(15) As applicable, establish an Enterprise Protection Risk Management system account via Secure Internet Protocol Router Network for conducting automated threat and vulnerability analysis;

(16) Coordinate with the designated command security policy SMEs and Team Leads for integration of OPSEC with Personnel Security, Information Security, Physical Security,

Industrial Security, Security Education and Training Awareness, Communications Security, and Anti-terrorism programs;

(17) Submit to HHQ, as tasked, input for inclusion in NAVSEA's to the biennial (OUSD (I&S)) OPSEC Status Report;

(18) Ensure command personnel complete initial and annual OPSEC refresher training. Coordinate with command Human Resources (HR) elements to ensure records of training completion are maintained. Solicit from HR, annual metrics of OPSEC training completion statistics and ensure data is readily accessible during compliance inspections and oversight assessments;

(19) Conduct annual OPSEC assessments and program reviews, and forward summary reports of results to the higher HQ OPSEC PM (after attaining review/concurrence of the Command Security Manager);

(20) As applicable, participate in the review process of official information considered for public release as directed by, and in support of, the command Public Affairs Office (PAO). Ensure decisions regarding release of information into the public domain will include a review by an appropriately designated and trained security professional. (NOTE: If reviewing and approving official information for public release, security personnel must complete the Interagency OPSEC Support Staff (IOSS) OPSEC and Public Release Decisions (OPSE-1500) training.);

(21) As applicable, conduct outreach to ensure family members are familiar with the significance of protecting critical information; and

(22) Maintain an OPSEC program continuity binder or a similar electronic repository. Ensure content is kept up-to-date and is readily accessible during compliance inspections and oversight assessments.

7. <u>OPSEC Security Education and Training Awareness</u>

a. As referenced above, all personnel assigned to OPSEC-related duties must satisfy both preparatory and sustaining OPSEC training per reference (c). OPSEC PMs of Level-II and Level-III programs will complete the following IOSS courses of training (or equivalent). At minimum, OPSEC Coordinators for Level-I programs must complete OPSE-1301 or equivalent training.

(1) OPSEC Fundamentals [OPSE-1301];

(2) OPSEC Analysis Course [OPSE-2380];

(3) OPSEC Program Management Course [OPSE-2390]; and

(4) OPSEC and Public Release Decisions [OPSE-1500] (if delegated the authority to review and recommend official information for public release, all OPSEC SMEs must complete OPSE-1500).

b. All newly assigned personnel must receive initial OPSEC awareness training within the first 30 days of arrival to the organization. It is recommended this training be conducted as part of an initial entry briefing or unit/organization newcomer's briefings. Annual OPSEC refresher training can be accomplished as a component of an overall command security refresher training briefing, however, an OPSEC SME must present this portion of training. For OPSEC to be effective, all NAVSEA personnel must be aware of OPSEC and understand how this complements traditional security programs. The goal is to emphasize the importance of sound OPSEC practices and to ensure each individual attains the requisite knowledge to safeguard critical information and reduce indicators.

c. Per reference (b), all personnel must complete OPSEC awareness training prior to being granted initial access to DON information technology (IT) systems and networks. Cybersecurity elements will establish processes and procedures to validate OPSEC training completion before authorizing network/system access. Additionally, personnel are required to observe policies and procedures governing the secure operation and authorized use of DoD IT, including operations security policies, per DoDI 8500.01, Cybersecurity.

d. Personnel designated as OWG members will complete OPSE-1301, OPSEC Fundamentals training (or equivalent) within 30 days of appointment.

NOTE: Above referenced education and training is offered by the National Security Agency's IOSS and can be accessed via the IOSS official website (https://www.iad.gov/ioss/). Equivalent OPSEC education and training is also offered by the various service components, the Defense Counterintelligence & Security Agency (DCSA)/Center for Defense and Security Excellence (CDSE) and the Joint OPSEC Support Element (JOSE).

8. OPSEC and Contracts

a. Per references (a) through (e), OPSEC requirements will be stipulated in all classified contracts. Additionally, OPSEC requirements will be considered for unclassified contracts as applicable. The OPSEC SME will be integrated at the beginning of the contract support process, to include providing associated OPSEC reviews of SOW, RFP or PWS for presence of critical or sensitive information. The originators of the request will coordinate with the OPSEC SME for review of contractual documents to determine if any specific OPSEC measures are required in the contract. This will ensure contractor understanding of the exact OPSEC measures to implement.

b. For classified contracts, the OPSEC SME will coordinate with the command's Industrial Security specialist during completion of a DD Form 254, Department of Defense Contract Security Classification Specification. The Industrial Security specialist completes the DD Form 254, which is used to convey security requirements in a classified contract. The Industrial Security specialist will review the SOW, RFP or PWS to ensure the appropriate security clauses and/or OPSEC language is contained therein to address the protection of classified information and critical information The Industrial Security specialist ensures the OPSEC measures contained in the SOW, RFP or PWS are also reflected on the DD Form 254. (Per references (a) through (e))

9. Public Release Review of Official Information

a. Official information considered for public release must undergo a security and content review, and clearance by a representative of the command's Security Department (e.g., OPSEC SME) prior to final release approval by the PAO. The PAO is required to solicit OPSEC SME assistance to accomplish a security and content review of official information before PAO approves for release into the public domain. Public release review considerations will be accomplished per references (c), (f) and (g).

b. Official information considered for initial public release will be routed, by PAO, through the Security Office for review and approval for release in sufficient time to allow potential security issues to be corrected by the submitter, while still meeting requested publication and distribution timelines.

c. NAVSEA Enterprise organizations without a designated local public release security review authority will route the information to the next higher command level for security content review.

d. Information submitted for public release will be safeguarded as CUI until a final public release approval determination is completed. Information submitted for public release review consideration must be appropriately protected during transmission such as being hand-carried or forwarded via first class or express mail. If forwarded electronically, information must be encrypted or only able to be accessed from a restricted site (e.g., iNAVSEA SharePoint, DoD Secure Access File Exchange (DoD SAFE), secure e-mail, etc.)

e. Only those security personnel who have completed the Interagency OPSEC Support Staff 'OPSEC and Public Release Decisions' [OPSE-1500] training, or equivalent, can authorize clearance and approval of official information for public release.

f. Offices coordinating information and materials for public release review consideration will maintain a system of record (e.g., log, spreadsheet, etc.) identifying each submission and release decision or recommendation. Ensure information is readily accessible during compliance inspections and oversight assessments.

10. Safeguarding and Protecting Critical Information

a. All designated critical information will be treated as need-to-know, or access must be for a lawful government purpose, and must be safeguarded. Unauthorized disclosure of identified NAVSEA critical information and indicators of sensitive activities, rather inadvertent or purposely, must be reported to the command Security Office and OPSEC PM immediately upon discovery.

b. Examples and sources of critical information and indicators disclosures can include:

(1) Overheard person-to-person conversations/discussions;

(2) Discussions via non-secure means (i.e., desk telephone);

(3) Print publications;

(4) Social network systems/social media;

(5) Official communications hosted via Internet Based Capabilities (IBC);

(6) Visually observed activities;

(7) Publicly accessible official web sites;

(8) Internet hosted;

(9) Unauthorized photo/video;

(10) Declassified information/materials; and

(11) Unauthorized access to controlled/restricted areas.

c. Personnel discovering or observing disclosures of CI or indicators, will implement or recommend corrective actions or mitigation efforts (e.g., measures and countermeasures), as necessary, to correct the discrepancy, in addition to reporting the disclosure to the command Security Office and OPSEC PM.

d. OPSEC measures and countermeasures can help preserve military capabilities by preventing adversarial exploitation of critical information. Countermeasures mitigate or remove vulnerabilities that point to or divulge critical information. OPSEC measures are used to prevent adversaries from observing potential indicators or sources of critical information and can minimize the risk of compromising information that could assist our adversaries in degrading friendly mission effectiveness. Examples of OPSEC measures and countermeasures to mitigate OPSEC disclosures (listing not all-inclusive):

(1) Command leadership support and backing of the OPSEC program;

(2) Development and dissemination of command CIIL;

(3) Command personnel complete OPSEC initial and annual refresher training;

(4) Integration of OPSEC into the contracting process;

(5) Immediately notify the OPSEC PM of presumed or actual OPSEC disclosures;

(6) Development and implementation of applicable OPSEC Plan documents;

(7) Responsible use of social media platforms to safeguard CI;

(8) Security content review of official information considered for public release;

(9) Utilize command web sites/pages for official business and in an official capacity;

(10) Ensure only authorized/approved photography on installation and facilities;

(11) Review command public accessible web pages for presence of sensitive information;

(12) Utilizing secure telecommunications (e.g. STE phone/fax, DODSAFE, etc.);

(13) Limit sensitive discussion in publicly accessible areas;

(14) Implement risk assessment/risk management procedures;

(15) Communications security monitoring of friendly unencrypted comms;

(16) OPSEC PM routine research for presence of official information in public domain;

(17) OPSEC PM cognizance of most current adversary threat reports and information; and

(18) Multi-Disciplinary Vulnerability Assessments.

e. Additionally, per the Information Security Oversight Office and National Security Presidential Memorandum 28, OPSEC is a designated category of CUI, and critical information is to be safeguarded per DoDI 5200.48, Controlled Unclassified Information.

11. Treaty on Open Skies Notifications. [NOTE: Per the U.S. Department of State announcement in the spring of 2020, the United States formally withdrew from the Open Skies Treaty affective November 2020.]

12. OPSEC Working Group (OWG). All NAVSEA commands with a designated OPSEC PM or Coordinator must have an active OWG. OWG meeting minutes will be compiled and maintained in a program continuity binder; or filed per local records management procedures. Each of the organization's key departments must assign a representative to participate in the OWG and assist the OPSEC PM in the execution of the command's OPSEC Program. Representatives should include, but not be limited to Security, Anti-Terrorism/Force Protection, Intelligence, Operations, Critical Infrastructure Protection, Public Affairs, Information Assurance/Cybersecurity and Freedom of Information Act representatives. Invite the Security Manager, Legal and applicable Contracting Officers or Contracting Officer Representatives to OWG meetings. Other members should include Public Affairs, Webmaster and Current Operations representatives, if assigned. Additional OWG member responsibilities include:

a. Assist the OPSEC PM in ensuring the accomplishment of all OPSEC related matters within their respective directorates or departments and provide necessary liaison to other OPSEC WG members in the accomplishment of the command's OPSEC program;

b. Attend regularly-scheduled OPSEC WG meetings;

c. Complete the OPSEC Fundamentals computer based training, or equivalent, within 30 days of appointment to the OWG and provide record of completion to the command OPSEC point of contact (POC).

d. Remain actively engaged in annual assessments, training, awareness campaigns, and other OPSEC tasks.

13. Critical or Sensitive Information in the Public Domain

a. Per references (d) and (h), OPSEC SMEs will periodically coordinate with the command's official web presence POCs, normally the Public Affairs Office Webmaster, to ensure critical or sensitive information is not posted to public facing official web sites, or hosted on IBC platforms supporting the command's official web presence.

b. Commands will develop tools or capabilities (i.e., checklist products) for periodically reviewing the command's official web page, in addition to conducting public domain research, to include the internet and social networking sites, for presence of OPSEC indicators, vulnerabilities, disclosures or sensitive information. Identify any OPSEC concerns to the web page host, OPSEC PM and/or command Security Manager. In addition, relay security concerns to NCIS, as warranted or applicable. Document these efforts, (such as compiling and maintaining summary reports), for review during compliance inspections or formal inquiries.

c. Command public facing web pages must not contain or display classified material, controlled unclassified information, command critical information, or information that could enable the user to infer this type of information.

14. TSCM Support. For those commands with Sensitive Compartmented Information Facilities, the Special Security Officer (SSO) will ensure OPSEC is implemented during TSCM planning and operations, per reference (i). Recommend SSO coordination with the command OPSEC SME, if necessary, for support in assuring applicable OPSEC processes and procedures are implemented to help safeguard TSCM activities.

15. Compliance with OPSEC Policies

a. Protecting and safeguarding command critical information is a key component of successful mission accomplishment. Our adversaries are continuously attempting to solicit, target, observe friendly critical information and indicators. Personnel who violate OPSEC policies and put command critical information at risk to disclosure and adversary collection risk potential disciplinary action, per reference (j). Violations of OPSEC policy can be reported to supervisors, OPSEC PM, command Security Manager, Contracting Officers, or NCIS liaisons.

b. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable Federal statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this instruction.

c. Civilian employees are subject to administrative penalties under applicable Federal statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this instruction.

16. 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 Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/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 records manager.

17. Review and Effective Date. Per OPNAVINST 5215.17A, SEA 00P will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

18. Forms. DD Form 254, Department of Defense Contract Security Classification Specification (APR 2018), cited in paragraph 8b, is available for download at: https://www.esd.whs.mil/Directives/forms/dd0001_0499/

W. J. GALINIS

Releaseability and Distribution:
This instruction is cleared for public release and is available electronically only via the NAVSEA Public Website located at http://www.navsea.navy.mil/Resources/Instructions/