



DEPARTMENT OF THE NAVY  
OFFICE OF THE SECRETARY  
1000 NAVY PENTAGON  
WASHINGTON DC 20350-1000

SECNAVINST 3070.2  
DUSN (P)  
5 May 16

SECNAV INSTRUCTION 3070.2

From: Secretary of the Navy

Subj: OPERATIONS SECURITY

Ref: See enclosure (1)

Encl: (1) References  
(2) Definitions  
(3) Department of the Navy Critical Information List  
(4) Roles and Responsibilities  
(5) Oversight  
(6) Operations Security: Detailed Self-Inspection Tool

1. Purpose. Establishes policy, procedures, and responsibilities for the Department of the Navy (DON) Operations Security (OPSEC) program per references (a) and (b).

2. Definitions. See enclosure (2).

3. Applicability. Applies to Total Force personnel, employed by, detailed or assigned to the DON, including Government Civilians (Appropriated and Non-Appropriated Funds), members of the active and reserve components of the U.S. Navy (USN) and U.S. Marine Corps (USMC); an expert or consultant performing services for the DON through a personnel appointment or a contractual arrangement and industrial or commercial contractor, licensee, certificate holder, or grantee, including subcontractors.

4. Policy

a. Pursuant to reference (a), the Secretariat, USN, and USMC shall maintain effective OPSEC programs that ensure coordination between public affairs, cybersecurity, security, operations, acquisition, intelligence, training, and command authorities and include mechanisms for enforcement, accountability, threat awareness, and the highest level of leadership oversight. OPSEC protects critical information to prevent an adversary from determining friendly intentions or

capabilities. Programs must endeavor to establish a proper balance between dissemination of information to families and the public, consistent with the requirement to protect critical information and maintain essential secrecy.

b. Commanders shall take all OPSEC measures required to prevent disclosure of critical information and protect essential secrets.

c. Commanders are required to establish, resource, and maintain effective OPSEC programs. A program consists of policies, manning, training, and equipping functions necessary for OPSEC planning and execution, and to ensure all personnel understand their responsibilities to protect essential secrecy. The maintenance and effectiveness of an OPSEC program is the responsibility of each Commanding Officer. Each program shall include, at a minimum: a designated OPSEC program manager and local instruction (policy and/or procedures specifically including requirements for oversight of subordinates); an effective OPSEC Working Group; a critical information list (CIL); training and awareness; family outreach; email, web, social media, and public affairs policies and strategies; as well as contract and acquisition review procedures. It shall also include processes to report and mitigate disclosures of critical information and potential disciplinary action against those who violate OPSEC policies. For operational Commands, the program shall also include measures and plans required to manage signatures of sensitive missions, programs, and/or operations.

d. Commanders are solely responsible for their OPSEC program(s). Management of the program can be delegated to officers O-3 or above or civilians GS-12 or higher, at a minimum, with sufficient authority and staff to manage the program for the Command. They must successfully complete OPSEC practitioner qualification training, and shall serve in the position for a minimum of 18 months. As a critical position, it must be filled at all times by a properly trained individual. OPSEC is an operations function, and therefore responsibilities should reside within the operations department. For Commands without an operations department, OPSEC program manager responsibilities shall be assigned to individuals who have significant authority in command operations. The OPSEC program manager shall have unimpeded access to the Commanding Officer.

This individual and the Commanding Officer shall ensure OPSEC is incorporated into all operations and activities. Due to the level of oversight over subordinate units and/or the sensitivity of the mission, Echelon I, II, and USMC Two-Star Commands and higher, require a full-time OPSEC program manager, unless waived per enclosure (4), paragraph 10b.

e. Program managers must be U.S. citizens and have a favorably adjudicated Single Scope Background Investigation completed within 5 years prior to assignment. Below Echelon II or USMC Two-Star Command equivalent, as well as for all OPSEC coordinators, a SECRET clearance is sufficient.

f. OPSEC is an operations function, and shall be integrated into all operational planning and coordinated with relevant military deception and other information operations programs.

g. OPSEC shall be coordinated and integrated into all other security disciplines (personnel, information, cybersecurity, acquisition, industrial, and physical, including law enforcement and antiterrorism/force protection).

h. DON organizations shall provide approved OPSEC training, including social media awareness, controlled unclassified information, and security review for public release pursuant to references (b) through (h), to all organization personnel upon accession. All DON personnel must also complete approved OPSEC awareness training on an annual basis and prior to receiving approval for access to DON networks. All training must be formally documented, maintained, and available on-line for higher Command review.

i. All Commanding Officers are responsible for oversight, guidance, and supervision over subordinate elements. Oversight and policy authority follow the administrative chain of command except if the organization is a deployable unit where it should follow the operational chain of command.

j. Decisions regarding release of information into the public domain shall include a review by an appropriately designated and trained OPSEC professional. Illustrative examples of such information include information released to Congress, budget documents, press releases, speeches,

newsletters, and official posts to web based resources pursuant to references (g) through (k). All public affairs professionals must be properly trained per references (a) and (b), and understand their command's CIL and at what level of detail its contents may be discussed.

k. Per reference (h), Public Affairs is responsible for the oversight and management of all content on official DON publicly-accessible Web presences. OPSEC, security, information security, and public affairs professionals are required to maintain on-going collaboration to ensure OPSEC is maintained on command social media profiles.

l. Research, development, test, and evaluation (RDT&E) activities as defined in references (i) and (j) are particularly vulnerable to compromise, both classified and controlled unclassified, and as such have an inherent requirement to implement OPSEC. Supply Chain Risk Management and Critical Program Information (CPI) protection principles must be adhered to per references (j) and (k), including OPSEC countermeasures.

m. OPSEC shall be used to evaluate the vulnerabilities of sensitive information and technology during all RDT&E activities and phases. Program managers at all levels should coordinate with their Acquisition Security/Research and Technology Protection Leads throughout the RDT&E life-cycle, especially regarding release of information into the public domain, prior to sensitive testing, and aboard or with operational units.

n. DON program executive officers, program, project, or product managers, and contracting officials shall include OPSEC as a stipulation in all contracts. All requirements packages must receive an OPSEC review at the start and completion of the contracting process to identify critical and/or sensitive information by the requiring activity OPSEC officer.

o. The DON CIL (enclosure 3) shall inform Command CILs, as well as enhance OPSEC guidance provided in public affairs policy (reference (h)). All Commands are responsible for developing their own unique CIL based upon threat information specific to their organization. Inclusion in the CIL in and of itself does not classify the information or preclude the information from public release. The Public Affairs Officer (PAO) and OPSEC

5 May 16

practitioner shall work with Command leadership to determine what level of detail to release publicly when the need for transparency outweighs the risk of disclosure.

p. Command critical information shall be transmitted in a manner that reduces the risk of aggregation and compromise. Where practicable, Secret Internet Protocol Router Network (SIPR) is the default method of transmission for critical information. When SIPR is not available, and the information is deemed by the Commander to be unclassified and not sensitive to on-going or planned operations, then encrypted unclassified transmission is authorized with the provision that OPSEC program is sufficiently robust and appropriate level of network monitoring is in place.

q. The Director of the Naval OPSEC Support Team (NOST) serves as a Senior Advisor to both Deputy Under Secretary of the Navy (Policy) (DUSN (P)) and Chief of Naval Operations (CNO) on all issues regarding OPSEC, safe use of social media, security review for public release, and related training.

5. Responsibilities. See enclosure (4).
6. Oversight. See enclosure (5).
7. Self-Inspections. Self-inspections may be facilitated using enclosure (6).
8. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of January 2012.
9. Forms and Reports. The reporting requirements contained in enclosure (4), paragraphs 3g, 8a, 9b, 10d, and the Annual OPSEC Report are assigned to Department of Defense (DoD) Report Control Symbol DD-INT(A)2228(3070).



JANINE A. DAVIDSON  
Acting

SECNAVINST 3070.2  
5 May 16

Distribution:

Electronic only, via Department of the Navy Issuances Web site  
<http://doni.documentservcies.dla.mil/>

**REFERENCES**

- (a) DoD Directive 5205.02E of 20 June 2012
- (b) DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual of 3 November 2008
- (c) DoDM 5200.01, Volume 4 DoD Information Security Program: Controlled Unclassified Information (CUI) of 24 February 2012
- (d) CJCSI 3213.01D Joint Operations Security of 7 May 2012
- (e) Joint Publication 3-13.3 Operations Security of 4 January 2012
- (f) NTTP 3-54M of March 2009
- (g) DoD Instruction 5230.29 of 13 August 2014
- (h) SECNAVINST 5720.44C CH-1
- (i) DoD Instruction 5230.24 of 23 August 2012
- (j) DoD Instruction 5200.39 of 28 May 2015
- (k) DoD Instruction 5200.44 of 5 November 2012
- (l) SECNAVINST 5430.7Q
- (m) SECNAVINST 5500.36
- (n) ALNAV 049/13, 171820Z July 2013
- (o) DoD Instruction 8550.01 of 11 September 2012
- (p) DoD Instruction 8500.01 of 14 March 2014
- (q) Foreign Intelligence Threat to the Department of the Navy series, Naval Criminal Investigative Service
- (r) Terrorist Threat to the Department of the Navy, series, Naval Criminal Investigative Service
- (s) DoD Instruction S-3604 Change 1 of 5 November 2013
- (t) DoDM 5105.21-V2 of 19 October 2012

## DEFINITIONS

1. Critical Information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.
2. Critical Information List (CIL). A list of critical information that has been fully coordinated within an organization and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.
3. Deception in Support of OPSEC (DISO). A DISO is a military deception activity that protects friendly operations, personnel, programs, equipment, and other assets against foreign intelligence security services (FISS) collection. The intent of a DISO is to create multiple false indicators to make friendly force intentions harder to interpret by FISS.
4. Essential Secrecy. The condition achieved from the denial of critical information to adversaries through the combined efforts of traditional security programs and the OPSEC process.
5. Essential Secrets. Aspects of friendly operations that, if compromised, would lead to adversary knowledge of exploitable conditions and a potential failure to meet the Commander's objectives and/or desired end-state.
6. OPSEC Coordinator. An individual trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC program manager or primary representative.
7. OPSEC Planner. A functional expert trained and qualified to plan and execute OPSEC.
8. OPSEC Program Manager. A full-time appointee or primary representative assigned to develop and manage an OPSEC program.
9. Protect. Actions taken to shield from exposure, damage, or destruction; to keep from harm, attack, injury, or exploitation; to maintain the status or integrity of.

**DEPARTMENT OF THE NAVY CRITICAL INFORMATION LIST**

1. OPERATIONS

a. Status and/or limitations of personnel, equipment, and weapons systems and key contingency concepts processes.

b. Operational command and control (C2) structure.

c. Standard operating procedure (SOP).

d. Identification, strength, and combat readiness posture of assigned forces.

e. Specific aspects and changes of Force Protection Conditions and/or Information Operations Conditions.

f. Details and locations of assets used in assigned missions including capabilities, the operational use of the assets, or their state of readiness.

g. Critical ship and/or activity or regional infrastructure nodes and/or links.

h. Alert status, response times, and schedules.

i. Exercise and/or inspection postures and results.

j. Policies and information regarding Rules of Engagement (ROE), to include the use of weapons and electronic or acoustic warfare systems. Air and ground tactics of U.S., allied, and/or coalition forces.

k. Mishap and/or accident information of a privileged nature.

l. Association of daily changing call signs (not international) and authentication procedures with unit designators.

m. Military Information Support Operations.

n. Military Deception Plans and Operations.

- o. Special Operations Forces and Unconventional Warfare.
- p. Special Weapons.
  - (1) Specific characteristics and capabilities of weapons.
  - (2) Doctrine for using various weapons.
  - (3) Indicators unconventional weapons will be employed.
  - (4) New weapons that are available or are being employed.
  - (5) Vulnerabilities and limitations in friendly weapons and weapons systems.
  - (6) Training related to Special Weapons and related systems.
- q. Results of adversary operations or battle damage against U.S. forces that could provide measures of effectiveness to the enemy.

## 2. PLANS

- a. Changes in wartime mission and/or tasking.
- b. Specific information of schedule of forces, equipment, or staging locations.
- c. Security classification of a classified operation, program, or project.
- d. Intent to mobilize before public announcement.
- e. Infrastructure reports.
- f. Evacuation routes, procedures, and rally points.
- g. Intended operational changes before public announcement.

### 3. COMMUNICATIONS AND INFRASTRUCTURE

- a. Capabilities, configuration, security measures, limitations, status, upgrades, or proposed changes related to communication systems, to include networks, transmission systems, relay stations, and associated equipment.
- b. Technical system architectures, capabilities, vulnerability information, and security assessment reports related to C2 systems or National Security Systems.
- c. Security, network architecture, topology, infrastructure, infrastructure design, and security risk assessment results of DON information technology.
- d. Location, schematics, capabilities, protection measures, vulnerabilities, and degradation of critical infrastructure.
- e. Network architecture diagrams or documents.
- f. Information revealing a communications security weakness or physical security weaknesses.
- g. Computer passwords, user IDs, and/or network access paths.
- h. Security authorization documentation including data provided to support Authorization to Operate or Connect decisions.
- i. Data collected in order to grant access to DON information technology, e.g., System Authorization Access Request forms.

### 4. INTELLIGENCE

- a. Intelligence sources or methods of gaining intelligence; analytical methods and processes.
- b. Intelligence assessments, maps, and locations of intelligence targets.
- c. Intelligence, surveillance, and reconnaissance resources.

- d. Counterintelligence capabilities.
- e. Intelligence gaps and limitations.

5. LOGISTICS

- a. Changes or shortages in equipment and/or command status that may impair mission capabilities.
- b. New equipment capabilities and/or limitations.
- c. Logistical posture of U.S. and allied forces.
- d. Consolidated Ship's Maintenance Plan.
- e. Port visit coordination.
- f. Airfield and rail operations, as well as, supply chains.

6. RDT&E/CPI

- a. Weapons systems development schedules (dates, times, locations).
- b. Emerging technologies applicable to new weapons systems.
- c. Computer software used in weapons systems development, testing, and evaluation.
- d. Specific contract criteria stated in a classified contract.
- e. Identification of Special Access elements within a contract or program.
- f. Specific Program Protection Plan implementation methods.
- g. Status, limitations, and/or development of weapons systems and design concepts and/or processes.
- h. Mishap and/or accident information of a test and evaluation exercise on emerging technologies.
- i. SOPs and other information related to test plans.

j. Intended areas where RDT&E experimentation and testing will be conducted.

k. Identification of strength, weakness, and combat readiness of emerging technologies.

l. Test and field experiment results.

7. BUDGET. Emergency requisition of funds (or unexpected loss of funding) disclosing details of daily and/or contingency or wartime operations.

8. INTERNET BASED MEDIA

a. Personal Identifying Information.

b. Blank Authorization Agreement (outlining definitive needs, gaps, limitations, and shortfalls).

c. Full organizational rosters and telephone directories.

d. Contingency plans and/or continuity of operations.

e. Architectural or floor plans, diagrams of an organizations building, property, or installation.

f. Pictures containing any security features, e.g., guard shack, barriers, uniformed guards, access badges, safes, locking mechanisms, weapons, etc., other than rank, rate, first name, last name, job title, and unit.

9. PERSONNEL

a. Personnel privacy issues and/or identifiers.

b. Identification and relation of command personnel with security badge, security clearances or access, and special projects.

c. Immunization, medical requirements, health status, and deficiencies.

d. Location, itineraries, and travel modes of key military and civilian personnel.

- e. Manpower gains or losses associated with contingency operations or exercise.
- f. Training deficiencies impairing mission accomplishment.
- g. Lists of personnel in the DON Cybersecurity workforce, e.g., DoD 8570 compliant.
- h. Lists of critical or executive personnel with mobile devices.

### **ROLES AND RESPONSIBILITIES**

1. The Under Secretary of the Navy is designated as the deputy and principal assistant to the Secretary of the Navy (SECNAV), and acts with the full authority of SECNAV in managing the DON, per reference (l).

2. DUSN (P) is the DON Security Executive and responsible for policy, program oversight, and resource advocacy for DON OPSEC programs and initiatives per references (m) and (n). DUSN (P) shall serve as the Chair of the DON OPSEC Advisory Group.

3. DUSN (P) Security Directorate (SD) is a field activity of DUSN (P) responsible for day-to-day execution of DUSN (P) OPSEC related responsibilities. Under the direction of DUSN (P), the DUSN (P) SD shall:

a. Serve as DUSN (P)'s Executive Agent in the execution of OPSEC related responsibilities.

b. Prepare an annual OPSEC report for submission to the Deputy Under Secretary of Defense for Intelligence and Security (DUSD (I&S)) per reference (a) and/or current policies.

c. Represent DUSN (P) on appropriate OPSEC related Office of the Secretary of Defense, inter- and intra-agency working groups, committees, and boards.

d. Manage all DON OPSEC related formal tasking.

e. Ensure OPSEC policies are integrated and coordinated.

f. Provide recommendations to DUSN (P) regarding resource advocacy.

g. Implement DON-level oversight and conduct annual program reviews of USMC and USN OPSEC programs for compliance with DON and DoD policy, to assess effectiveness and to identify any resource or other gaps, keeping DUSN (P) informed.

h. Conduct random inspections of USMC, USN, and other DON OPSEC programs as required, keeping DUSN (P) informed.

i. Designate and promulgate OPSEC products approved to meet mandatory OPSEC training requirements.

j. Advocate for the establishment, resourcing, and implementation of OPSEC training for all DON personnel, as well as assess the effectiveness of these programs. This includes DON mandatory OPSEC training and additional OPSEC awareness products as necessary.

4. Assistant Secretary of the Navy (Manpower and Reserve Affairs) shall ensure that OPSEC awareness training and culture is integrated into individual and unit training programs as required.

5. Assistant Secretary of the Navy (Research, Development, and Acquisition) (ASN (RD&A)) shall ensure that OPSEC is employed to protect supply chain, design, and testing from potential adversaries. ASN (RD&A) shall:

a. Maintain procedures for OPSEC review of contracts prior to public release.

b. Develop procedures to reduce the threat of aggregation from the release of programmatic and contractual information.

c. Ensure all contract personnel receive training sufficient to protect essential secrets.

d. Annually review Navy System Command programs to ensure compliance with this instruction.

e. Ensure all contract management personnel receive appropriate OPSEC training.

f. Appoint in writing, an OPSEC program manager, to provide oversight over subordinate programs and serve on the DON OPSEC Working Group.

6. Department of the Navy/Assistant for Administration shall ensure that all members of DON Secretariat staff receive OPSEC training annually.

7. Navy Chief of Information (CHINFO) shall:

a. Ensure OPSEC considerations are incorporated into all DON public affairs release-of-information processes, guidance, and training per reference (a).

b. Provide a representative to DON OPSEC Working Group.

8. Department of the Navy Chief Information Officer (DON CIO) shall:

a. Include completion of initial and annual DON OPSEC training as a component of DON Network access policy per references (o) and (p).

b. Provide a representative to the DON OPSEC Working Group.

9. Director, Naval Criminal Investigative Service (NCIS) shall:

a. Provide a representative to the DON OPSEC Working Group.

b. Publish an annual assessment of the Foreign Intelligence Threat to the DON and the Antiterrorism Threat to the DON that provide OPSEC managers information on foreign intelligence priorities, targets, tactics, techniques, procedures, and trends affecting DON interests (references (q) and (r)).

c. Ensure relevant installation or activity specific counterintelligence information developed by NCIS is made available to support OPSEC managers.

10. CNO and Commandant of the Marine Corps (CMC) shall:

a. Establish an effective OPSEC program pursuant to provisions of this policy, and:

b. Have on staff a full-time OPSEC program manager (O-4/5 or civil service equivalent), and ensure a professional full-time OPSEC manager at the O-3 or GS-12 level at Echelon II commands. Waivers may be submitted to CNO and CMC for Commands without a significant operational responsibility or that do not engage directly in program or mission support. Those programs can fulfill this requirement with a part-time program manager or coordinator, with clearance requirements equivalent to Echelon III or below.

- c. Issue and maintain an OPSEC instruction and/or order providing specific guidance regarding organizations and operations.
- d. Provide a copy of their annual review of USN and USMC OPSEC programs to DUSN (P) for consolidated submission to DUSD (I&S).
- e. Have overall responsibility for their Service's OPSEC policy, oversight, resourcing, training, reporting, and implementation of responsibilities.
- f. Ensure OPSEC is a command emphasis item and include OPSEC effectiveness as a stand-alone evaluation objective for all operations, exercises, and activities.
- g. Ensure a process is in place to report disclosures of critical information in order to implement appropriate mitigation measures. Commanders shall ensure personnel are aware that failure to follow OPSEC guidance can result in disciplinary action, and shall hold accountable personnel who violate OPSEC policies.
- h. Conduct required OPSEC and Internet-based Capabilities assessments and/or surveys per references (a) and (d).
- i. Submit a Program Objective Memorandum to provide sufficient resources to the NOST and Marine OPSEC Support Team (MOST) to ensure effective implementation of their missions.
- j. Ensure annual standardized and unit-specific OPSEC training and education are conducted and documented for all Service Members, civilians, and contractors.
- k. Ensure service personnel receive OPSEC training starting with accession and orientation programs. Ensure deploying personnel and families receive additional OPSEC training to decrease vulnerabilities and reduce indicators per references (a) and (b).
- l. Ensure organizational OPSEC lessons learned are captured and disseminated.

m. Ensure OPSEC is embedded into all acquisition programs and contracts, as well as ensure all defense contractors abide by DoD and DON OPSEC requirements.

n. Ensure OPSEC and social media policy is emphasized to Family Readiness support program and incorporated into Ombudsman training. This emphasis shall not be limited to periods of deployment or mobilization.

o. Develop and issue a policy governing DISO pursuant to reference (s).

p. Man, train, and equip a cadre of certified OPSEC planners sufficient to meet Combatant Commander and other operational requirements. Additionally, ensure that each element that conducts operational planning includes at least one certified OPSEC planner.

q. Ensure mission essential tasks (METs) for OPSEC and related functions are incorporated into all "assess-train-certify" related documentation and requirements. These METs shall be an independent evaluation category, and not subordinated to other disciplines, e.g., Information Operations or Electronic Warfare.

r. Ensure the OPSEC program addresses all personnel with access to sensitive and/or critical information, e.g., Sailors and Marines, civilians supporting the military, contractors, family members, local national employees, and all other individuals who have access.

s. Ensure that a Command has an effective and compliant OPSEC program prior to being considered for Fleet or Marine operational awards (such as the Navy "E" series). Absence of an OPSEC program shall be cause for disqualification.

t. Ensure OPSEC is incorporated into all contractual requirements and documents, both classified and unclassified, involving sensitive and/or critical information.

u. Ensure appointed OPSEC program manager(s), officer(s), and/or coordinator(s) are provided with the opportunity and resources to attend OPSEC-related courses, conferences, and meetings.

v. Ensure the review process for public release of information includes an OPSEC review to prevent the release of sensitive and/or critical information which includes U.S. information that is determined to be exempt from public disclosure per all applicable laws and regulations.

w. Ensure all OPSEC program manager(s), officer(s), coordinator(s), PAOs, Freedom of Information Act (FOIA) officers, speechwriters, contracting specialists, Foreign Disclosure Officers, and personnel responsible for the review and approval of information intended for public release receive OPSEC training tailored to their duties.

x. Resource a capability to conduct routine reviews of unit and/or organization websites to ensure protection of essential secrets, and to ensure that the content remains relevant, appropriate, and devoid of critical and/or sensitive information identified on the CIL. All OPSEC reviews will be documented.

y. Develop and issue procedures to ensure USN and USMC entities do not make critical and sensitive information available on publicly-accessible websites.

z. Ensure all OPSEC programs are reviewed annually by both the designated program manager and coordinator.

aa. Conduct an OPSEC Assessment, previously referred to as a "Survey" at least once every 3 years, of programs down to the Echelon II level.

ab. Provide a representative to the DON OPSEC Working Group.

ac. Ensure appropriate OPSEC training and accountability documentation is required for all individuals prior to granting access to any DON Nonsecure Internet Protocol Router Network (NIPR), SIPR, or other information technology.

ad. Within 120 days of issuance of this instruction, provide DUSN (P) SD an assessment of the effectiveness of USN and USMC OPSEC programs, as defined in this instruction. In

SECNAVINST 3070.2  
5 May 16

this assessment, document program deficiencies, resource shortfalls, and what would be required to bring OPSEC programs into full compliance with this instruction.

ae. Review and approve waivers for requirements pursuant to paragraph 4d of this instruction for Commands with minimal operational requirements.

**OVERSIGHT**

1. A DON OPSEC Advisory Group shall provide governance for all relevant Secretariat, USN, and USMC activities. The group shall be chaired by DUSN (P). Standing membership includes representatives from DON CIO, ASN (RD&A), OPNAV (N2N6, N314, N3N5), HQ Marine Corps Plans, Policies, and Operations, NOST, MOST, CHINFO, the Office of Marine Corps Communications, NCIS, the Office of the Naval Inspector General, Intelligence Support Division, and other representatives and experts deemed necessary to conduct relevant deliberations.

2. DON, in coordination with the CNO, CMC, and other key stakeholders, shall conduct random inspections of subordinate OPSEC programs. These inspections may be conducted during regularly scheduled or other command review events. Self-inspections may be facilitated using enclosure (6).

**OPERATIONS SECURITY:  
DETAILED SELF-INSPECTION TOOL**

**1.0 ECHELON II COMMANDS ONLY AND USMC TWO STAR EQUIVALENTS**

- 1.1 Does the OPSEC program manager, coordinator, or planner provide OPSEC policy and planning guidance to subordinate units? Are they serving in their OPSEC capacity full-time? Do they have a TS/SCI clearance? **References (Ref):** Reference (d), Encl. A, pg. A-10, para 7a; SECNAVINST 3070.2, para 4d, 4i

**If yes, review past examples of how coordination occurred.**

- 1.2 Does the OPSEC program manager, coordinator, or planner enter OPSEC lessons learned into the appropriate lessons learned database(s), which is available to all unit OPSEC practitioners? **Ref:** Reference (b), Encl. 4, pg. 18, 1b(1)(c)

**If yes, review past examples of how this was/is accomplished.**

- 1.3 Does the organization have an OPSEC support capability that provides for program development, training, assessments, surveys, and readiness training? **Ref:** Reference (a), Encl. 2, pg. 7, para 11h; Reference (a), Encl. 2, pg. 8, para 13c

**If yes, who is the point of contact (POC), how is support coordinated and tasked? On average, how often is this capability engaged by this command annually?**

- 1.4 Is the OPSEC process incorporated into operations, exercises, activities, system development, and test and evaluations? Did the command create an OPSEC Tab for each Operations Order developed by the organization? **Ref:** Reference (d), Encl. A, pg. A-6, para 6g; SECNAVINST 3070.2, para 4d, 4f

**If yes, review documentation from past evolutions illustrating OPSEC as a consideration within the plan, or OPSEC plan supporting said event.**

- 1.5 Was a response to the Annual DUSD (I&S) OPSEC Questionnaire received from all subordinate commands, consolidated, and reported to (USN) USFLTCYBERCOM / (USMC) HQMC OPSEC Program Manager?

**If yes, review documentation.**

- 1.6 Does the command maintain an up-to-date list of immediate subordinate commands and their OPSEC POCs?

**If yes, review documentation.**

## **2.0 ALL COMMANDS**

- 2.1 Does the command maintain a continuity binder and ensure OPSEC policies, programs, and plans are executed and evaluated through regular assessments? **Ref:** Reference (d), Encl. A, pg. A-10, para 7b(8)

**If yes, review content for pertinence.**

- 2.2 Has the organization appointed in writing an OPSEC program manager, coordinator, or planner? Does the OPSEC program manager have at least a Secret clearance? **Ref:** SECNAVINST 3070.2, para 4c

**If yes, review documentation.**

- 2.3 Is the OPSEC program manager, coordinator, or planner someone who is familiar with the operational aspects of the activity including the supporting intelligence, counterintelligence, and security countermeasures? **Ref:** SECNAVINST 3070.2, para 4d

**If yes, review documented examples.**

- 2.4 Has the OPSEC program manager, coordinator, or planner completed the appropriate training? **Ref:** SECNAVINST 3070.2, para 4d

**If yes, inspect graduation certificate.**

- 2.5 Does the OPSEC program manager, coordinator, or planner lead internal local OPSEC Working Group meetings? Does the OPSEC Working Group include representatives from all major sections, departments, divisions, or tenant commands as applicable, as well as public affairs, information security, web administrators, and contracting representatives? **Ref:** Reference (d), Encl. A, pg. A-11, para 7b(13); SECNAVINST 3070.2, para 4c

**If yes, review minutes of OPSEC Working Group.**

- 2.6 How often does the OPSEC Working Group meet and what are the actions that the OPSEC Working Group performed? Are working group minutes maintained (see above)?

**If yes, review documentation.**

- 2.7 Does the command have an OPSEC policy or instruction in place? **Ref:** Reference (d), Encl. A, pg. A-5, para 6a; SECNAVINST 3070.2, para 4c

**If yes, review policy or instruction for pertinence and is it signed by the commander?**

- 2.8 Does the OPSEC instruction(s) establish formal review procedures for relevant OPSEC concerns? **Ref:** SECNAVINST 3070.2, para 4c

**If yes, request a demonstration of the procedures.**

- 2.9 Does the command have a Critical Information List (CIL) that has been fully coordinated within the organization and approved by the senior decision maker? Has it been updated or at least verified within the past year? **Ref:** Reference (b), Append. 1 to Encl. 3, pg. 13, para 2a(5); Reference (b), Encl. 3, pg. 10, para 3a(2)(a); SECNAVINST 3070.2, para 4c, 4o

**If yes, review documentation.**

- 2.10 Is the CIL made available and used by all personnel in the organization? **Ref:** SECNAVINST 3070.2, para 4c, 4o

**If yes, inspect locations of CIL.**

2.11 Has a risk analysis and vulnerability analysis been performed? **Ref:** SECNAVINST 3070.2, para 4c

**If yes, review documentation.**

2.12 Are OPSEC measure and/or countermeasures in place to protect sensitive and critical information? Is there a process in place to review their efficacy? **Ref:** SECNAVINST 3070.2, para 4c

**If yes, review documentation.**

2.13 Does the command provide OPSEC orientation and awareness training to assigned personnel as well as ensuring OPSEC awareness training is conducted at least annually? **Ref:** Reference (d), Encl. A, pg. A-7, para 6i(1); Reference (d), Encl. B, pg. B-5, para 10a; Reference (b) Encl. 7, pg. 35, para 3; SECNAVINST 3070.2, para 4h

**If yes, review presentations and attendance rosters.**

2.14 Does the command ensure classified and unclassified contract requirements properly reflect OPSEC responsibilities and that these responsibilities are included in contracts when applicable? **Ref:** Reference (b), Encl. 6, pg. 32, para 2; Reference (d), Encl. A, pg. A-6, para 6f; SECNAVINST 3070.2, para 4n

**If yes, inspect and review example.**

2.15 Does the OPSEC program manager, coordinator or planner provide OPSEC guidance and oversight to subordinate units, if applicable? Has the OPSEC program manager conducted an OPSEC assessment of their subordinate commands, if applicable, within the past year? **Ref:** SECNAVINST 3070.2, para 4i

**If yes, seek feedback from subordinate unit(s) OPSEC program manager, coordinator, or planner.**

2.16 Does the organization ensure OPSEC is included in activities that prepare, sustain, or employ U.S. Armed Forces during war, crisis or peace, including research, development, test and evaluation; special access programs; DoD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and release of information to the public, when applicable?  
**Ref:** Reference (b), Encl. 2, pg. 7, para 6a(1)

**If yes, review past examples.**

2.17 Does the OPSEC program manager, coordinator or planner ensure OPSEC assessments and surveys are conducted per the DoD policy? **Ref:** Reference (b), Encl. 4

**If yes, review past assessments and/or surveys.**

2.18 Does the command maintain past assessments, at a minimum, the last annual assessment?

**If yes, review assessments.**

2.19 When applicable, has the command provided OPSEC training for the pertinent family readiness organizations and unit family members? **Ref:** Reference (d), Encl. A, pg. A-8, para 6i(4); Reference (d), Encl. B, pg. B-6, para 10d; SECNAVINST 3070.2, para 4c

**If yes, review presentations.**

2.20 Does the OPSEC program manager conduct threat analysis with threat assessment organizations, i.e. NCIS, for each separate mission or project to identify potential adversaries, both domestic and foreign, whenever necessitated by changes in tasking, environment, etc.?  
**Ref:** Reference (b), Append. 1 to Encl. 3, pg. 13, para 2b

**If yes, review past assessments and POC information.**

2.21 Does the OPSEC program manager conduct open search research on the unit to include: social networking sites, bulletin boards, news releases, etc. for OPSEC indicators, vulnerabilities, or disclosures?

**If yes, review process used and any findings.**

2.22 Does the command have a shred, personal electronic device and other supporting policies? **Ref:** Reference (e), Ch. III, pg. III-8, para 4d (10)

**If yes, review policies.**

2.23 Is OPSEC integrated into the Command's policies on the personal use of email, the internet, and social media? Is an enforcement regime in place? If so, has it been communicated effectively to all personnel with access to the network? **Ref:** Reference (d), Encl. A, pg. A-7, para 6h; Reference (d), Encl. A, pg. A-8, para 6j; SECNAVINST 3070.2, para 4a

**If yes, review policies.**

2.24 Do OPSEC, Security, Intelligence, Information Technology, and Public Affairs professionals communicate and collaborate on a routine basis? Is OPSEC integrated in Command decisions for release of information into the public domain? Is it included in the unit's OPSEC instruction or policy? **Ref:** Reference (b), Encl. 5; Reference (d), Encl. A; SECNAVINST 3070.2, para 4a

**If yes, review policies.**

2.25 Is OPSEC integrated throughout the contracting and acquisition cycle? Have contracting and acquisition personnel received appropriate training? Is there an OPSEC review process in place for contracts? **Ref:** Reference (d), Encl. A, pg. A-6, para 6f; Reference (b) Encl. 6, pg. 32, para 2; SECNAVINST 3070.2, para 4l, 4m

**If yes, review policies.**

2.26 Does the Command receive threat information tailored to their specific needs? If so, where does the information come from? How frequently is it updated and how is it provided to unit personnel?

**If yes, review briefing and training rosters.**

2.27 Is OPSEC integrated into antiterrorism/force protection planning?

**If yes, review policies.**

2.28 Does the command provide and document OPSEC training prior to granting individuals access to any DON NIPR, SIPR, or other information technology? **Ref:** SECNAVINST 3070.2, pg. 3, para 4h

**If yes, review training documentation.**

2.29 (If Command has Sensitive Compartmented Information Facilities) Does the Command include OPSEC requirements into Technical Surveillance Countermeasures support? **Ref:** Reference (t), Encl. 4, pg. 41, para 2

**If so, show documentation.**