SECNAV INSTRUCTION 3070.2A

From: Secretary of the Navy

Subj: OPERATIONS SECURITY

Ref: See enclosure (1)

Encl: (1) References
      (2) Definitions
      (3) OPSEC Program Manager Requirements
      (4) OPSEC Working Group Requirements
      (5) OPSEC Instruction Requirements
      (6) OPSEC Plan Template
      (7) OPSEC Program Checklist
      (8) Roles and Responsibilities

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

2. Cancellation. SECNAVINST 3070.2.

3. Definitions. See enclosure (2).

4. Applicability. This instruction applies to the Office of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all U.S. Navy (USN) and U.S. Marine Corps (USMC) installations, commands, activities, field offices, and all other organizational entities within the DON. This includes all DON personnel (military and civilian), as well as supporting contractor employees.

5. Policy

   a. Pursuant to reference (a), the Secretariat, USN, and USMC shall maintain effective OPSEC that ensures coordination between public affairs, all security disciplines, 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 maintain essential secrecy.

c. Commanders are required to establish, resource, and maintain effective OPSEC. OPSEC includes 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 OPSEC is the responsibility of each commanding officer. Each command shall include, at a minimum:

(1) A designated OPSEC program manager meeting the criteria listed in enclosure (3). The program manager shall familiarize themselves with the requirements and procedures of references (a) through (e), their service-level OPSEC instruction as applicable, and any additional guidance from their chain of command.

(2) An effective OPSEC working group in accordance with the guidance of enclosure (4).

(3) A tailored, command-specific training program that ensures all assigned personnel are aware of the contents of their Critical Information and Indicators List (CIIL) and their specific responsibilities for safeguarding critical information. All assigned personnel must receive OPSEC training as part of their onboarding process prior to approving personnel for access to DON networks, and at least annually. This training shall include, at a minimum, the unit’s CIIL; social media awareness and vulnerabilities; local threats; how to protect, transmit, and destroy controlled unclassified information; risks and guidance pertaining to geolocation-capable devices, applications, and services; and OPSEC review procedures for public release. All training must be formally documented, maintained, and available online for higher command review. Family outreach shall also be performed to educate the families of assigned personnel about OPSEC principles and concerns.
Additional guidance on OPSEC family outreach can be found in reference (e), chapter 9 and appendix M.

(4) A local OPSEC instruction in accordance with the guidance of enclosure (5).

d. Although recommended for all commands, operational commands that conduct sensitive missions, operations, or testing and evaluation must additionally develop an OPSEC plan per the template of enclosure (6) to manage signatures that reveal critical information. OPSEC plans at a minimum will list the critical information, associated indicators of the critical information, and assigned OPSEC measures for each indicator. An overall OPSEC plan shall be augmented as needed by OPSEC operations plans specific to planned involvement in specific operations.

e. OPSEC is an operations function, and shall be integrated into all operations planning and coordinated with relevant military deception plans and other information-related capabilities (IRCs). OPSEC shall additionally be incorporated into the Operational Risk Management (ORM) framework, and risks to critical information shall be reviewed and mitigated as part of the ORM process.

f. Commanders are responsible for oversight, guidance, and supervision over both their own OPSEC and that of their subordinate elements. Each command shall conduct an annual OPSEC assessment per reference (a), which may consist of either a documented self-assessment, an Inspector General inspection, or a higher headquarters assessment. Additionally, commands shall inspect subordinate commands for OPSEC compliance and effectiveness at least once every three years. Assessments shall include a review of information released to the public for critical information to include unit websites and social media accounts, and may include open source research. Oversight and policy authority follow the administrative chain of command except for deployable units, where it follows the operational chain of command. The checklist provided in enclosure (7) may be used to facilitate the administrative portion of an OPSEC assessment or may be augmented or replaced as appropriate by service or command guidance. Checklists provided in reference (e), appendices A and P may also be helpful in implementing OPSEC best practices.
g. All information considered for release into the public domain shall include a review in accordance with the appendix to enclosure (3) of reference (f), and shall involve an appropriately designated and trained OPSEC professional. All public affairs professionals must be properly trained per references (a) and (b) and understand their command’s CIIL sufficiently to determine what details of the command’s activities may be shared with the public. The Public Affairs Officer (PAO) and OPSEC program manager shall work with command leadership to determine when the need for public transparency outweighs the risk of disclosure. Additional guidance on the relationship between OPSEC and public affairs can be found in reference (e), chapter 8. Additional guidance on OPSEC considerations for use of the Internet and social media can be found in reference (f), chapters 6 and 10 and appendix K.

h. Research, development, test, and evaluation (RDT&E) activities and documentation as defined in references (g) and (h), comprising both classified and controlled unclassified information, are particularly vulnerable to disclosure and compromise and as such must exercise particular care and attention in implementing robust OPSEC. Supply Chain Risk Management and Critical Program Information (CPI) protection principles must be adhered to per references (h) and (i), including OPSEC measures and countermeasures, and OPSEC shall be considered in all Program Protection Plans (PPPs).

i. 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 respective Systems Command (SYSCOM) leads for program protection 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.

j. DON program executive officers, program, project, or product managers, and contracting officials shall include OPSEC considerations 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 program manager. Additional guidance on OPSEC considerations in contracts can be found in reference (e), appendix J.
k. Critical information shall be transmitted in a manner that reduces the risk of aggregation and compromise. Where practicable, a classified network (either data or phone) is the preferred method of transmission for critical information. When a classified network is not available and the information is not sensitive to ongoing or planned operations, then it may be transmitted over an unclassified network so long as it is encrypted. Unencrypted transmission of critical information over an unclassified network is not authorized.

1. The Naval OPSEC Support Team (NOST) and Marine OPSEC Support Team (MOST) are designated as the service OPSEC support elements for the Navy and Marine Corps respectively, per reference (a). In that capacity they serve as advisors to the Deputy Under Secretary of the Navy (DUSN) as well as CNO and CMC respectively on all issues related to OPSEC and related support to their services as required. Requests for OPSEC support from the NOST and MOST can be sent to OPSEC@navy.mil and MOST@mcia.osis.gov, respectively.

6. **Responsibilities.** See enclosure (8).

7. **Records Management.** Records created as a result of this instruction, regardless of media and format, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page (https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx).

8. **Reports.** The requirements contained in enclosure (5), paragraph 1d and enclosure (8), paragraph 8 are exempt from reports controls per part IV, paragraph 7n of reference (j).

THOMAS B. MODLY
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances Web site https://www.secnav.navy.mil/doni/.
REFERENCES

(a) DoDD 5202.02E, DoD Operations Security (OPSEC) Program of 20 June 2012
(c) CJCSI 3213.01D, Joint Operations Security of 7 May 2012
(e) NTTP 3-13.3M/MCTP 3-32B, Operations Security (OPSEC) of September 2017
(f) DoD Instruction 8550.01, DoD Internet Services and Internet-Based Capabilities of 11 September 2012
(g) DoD Instruction 5230.24, Distribution Statements on Technical Documents of 23 August 2012
(i) DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) of 5 November 2012
(j) SECNAV M-5214.1, Department of the Navy Information Requirements (Reports) Manual of December 2005
(k) SECNAVINST 5500.36, Department of the Navy Security Enterprise of 19 May 2015
(l) ALNAV 049/13, 171820Z July 2013
(m) Foreign Intelligence Threat to the Department of the Navy, series, Naval Criminal Investigative Service
(n) Terrorist Threat to the Department of the Navy, series, Naval Criminal Investigative Service
(o) DoD Instruction S-3604.01, DoD Military Deception of 11 March 2013
DEFINITIONS

1. **Operations Security** (OPSEC). A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

2. **Essential Secrecy.** The condition achieved from the denial of critical information and indicators to adversaries through the combined efforts of the OPSEC program and traditional security programs.

3. **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.

4. **Indicator.** Data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities.

5. **OPSEC Measure.** Planned action to conceal or protect critical information and indicators from disclosure, observation, or detection and protect them from collection; generally defensive in nature.

6. **OPSEC Countermeasure.** Planned offensive action taken to affect collection, analysis, delivery, or interpretation of information that impacts content and flow of critical information and indicators.

7. **Critical Information and Indicators List** (CIIL). A list of critical information and indicators for a specific command or organization.
8. **OPSEC Plan.** A plan that matches critical information to associated indicators, and assigns OPSEC measures or countermeasures as appropriate to reduce vulnerabilities and mitigate risk.

9. **OPSEC Operations Plan.** An augment to a standing OPSEC plan that provides specific measures and countermeasures to be applied by a unit during a specific operation. It may be generated as an annex to a Joint Operation Planning and Execution System plan or as a local document endorsed by the commander.

10. **Deception in Support of OPSEC (DISO).** DISO is a military deception planned and executed to protect the security and secrecy of friendly operations, personnel, programs, equipment, and other assets from foreign intelligence entity (FIE) collection.

11. **OPSEC Program Manager.** An appointee or primary representative assigned to develop and manage an OPSEC program.

12. **OPSEC Coordinator.** An individual trained in OPSEC who works in coordination with the OPSEC program manager or primary OPSEC representative.

13. **OPSEC Planner.** A functional expert trained and qualified to plan and execute OPSEC.

14. **Open Source Research.** Monitoring publically available information to identify potential disclosures of critical information and indicators. Open source research does not produce intelligence.
OPSEC PROGRAM MANAGER REQUIREMENTS

1. Commanders are ultimately responsible for the compliance and effectiveness of their OPSEC program. Management of the program can be delegated to a program manager designated in writing and with unimpeded access to the commanding officer who meets the following criteria:

   a. A military officer O-3 or above or civilian GS-12 or above, with sufficient authority and staff to manage the program for the command. For commands below the two-star level, a Chief Warrant Officer or Limited Duty Officer of any grade is also acceptable.


   c. A graduate of appropriate OPSEC program manager training offered by a service OPSEC Support Element (e.g., the Navy OPSEC Support Team) or the Interagency OPSEC Support Staff, or with a quota to complete training within 90 days of designation.

   d. A projected rotation date at least 18 months from the date of designation. For civilians without an official projected rotation date, they must have a reasonable, good faith expectation of continuing in the position for at least 18 months.

   e. Assigned to the operations department where applicable, or otherwise in a position or department with direct involvement in and information regarding the execution of key command missions, functions, and tasks.

   f. Possessing clearance and access appropriate to the mission and function of the organization allowing unimpeded performance of duties, and at minimum a Secret clearance per reference (c), enclosure (a), paragraph 7a.

   g. Shall not be a Public Affairs Officer (PAO) or member of the public affairs staff, to prevent any possible conflict of interest.

   h. For commands at the two-star level or above, the OPSEC program manager must be assigned full-time and not as a collateral duty, unless waived per enclosure (8), paragraph 10e.
2. Based on the requirements above, for afloat or deploying commands the most appropriate designee for OPSEC program manager will tend to be the operations officer (or N3, S3, or G3 as appropriate), as they will have the requisite grade, authority, access, and placement to effectively implement OPSEC. Owing to the number of duties and responsibilities typically placed on these persons, an additional assistant OPSEC program manager may also be appointed by the program manager with the requirement that they be E-6 or higher, and have attended an approved OPSEC program manager's course.

3. Because contractors do not have authority over U.S. military and government personnel and cannot represent the position of the U.S. Government, contract employees will not be assigned as a command’s OPSEC program manager or coordinator. They can perform OPSEC duties in a supporting capacity under the supervision of a government employee or servicemember.
OPSEC WORKING GROUP REQUIREMENTS

1. The working group shall convene at least quarterly to assist the OPSEC program manager in applying the five-step OPSEC process to the command per reference (e), chapter 3. As such it should assist the designated OPSEC program manager in generating and updating their CIIL, understanding the evolving threat to critical information, assessing vulnerability and risk, and implementing effective OPSEC measures and countermeasures with the involvement of all elements of a command.

2. An OPSEC working group shall include representatives of all key command components, departments, or functions. Per reference (c), enclosure A, paragraph 7b(13), it shall include where applicable representatives for:
   
   a. security,
   
   b. anti-terrorism/force protection,
   
   c. intelligence,
   
   d. critical infrastructure protection,
   
   e. public affairs,
   
   f. information assurance,
   
   g. and FOIA.
   
   h. where applicable, it should additionally include representation from the command technical authority and the Naval Criminal Investigative Service (NCIS). In the absence of a representative from NCIS an alternative counterintelligence representative should attend.

3. Minutes shall be kept of OPSEC working group meetings and retained for review.
OPSEC INSTRUCTION REQUIREMENTS

1. All commands shall publish a local OPSEC instruction to direct the implementation of higher guidance and the execution of the OPSEC process detailed in reference (e), chapter 3, as tailored to the specific command. The command instruction should include:

   a. A command CIIL tailored to specific command functions through application of the OPSEC process detailed in reference (e), chapter 3. Commands responsible for many disparate functions and especially those with geographically separated components should consider separate CIILs for each function or location along with an assigned OPSEC coordinator. For research and development activities, the PPP shall also be consulted as a resource in developing a CIIL. The CIIL must not be static and should be updated regularly as the situation or mission evolves, and at least annually per reference (c), enclosure (a), paragraph 7b(4). Additional guidance on elements to include in a CIIL can be found in reference (e), appendices B, C, and Q.

   b. Policy and guidance for the establishment of an effective command OPSEC working group as described in paragraph 5c(2) above.

   c. Policy and guidance for the effective conduct of command OPSEC training as described in paragraph 5c(3) above.

   d. Policy and guidance for the reporting and mitigation of disclosures of critical information and for potential disciplinary action against those who violate OPSEC policies. OPSEC violations should at minimum be documented and reported to the commanding officer, and to higher headquarters upon request.

   e. Policy and guidance for approved methods for transmission and disposal of critical information.

   f. Policy and guidance for incorporation of OPSEC into contracts and acquisitions, where applicable.

   g. Policy and guidance for oversight of the OPSEC programs of subordinate commands, where applicable.
OPSEC PLAN TEMPLATE

OPERATIONS SECURITY (OPSEC) PLAN

FOR

XXXX

Date

Overall document Classification is:
Classified By:
Derived From:
Declassify on:
COMMANDER XXX OPERATIONS SECURITY (OPSEC) PLAN FOR XXX OPERATIONS

References:

a. List all applicable references

1. SITUATION.
   a. General. Describe the conditions that exist to warrant the development of the plan.
   b. Adversary. Describe the enemy situation that provided the impetus for this plan. Describe the specific adversary FIE capabilities that can detect and observe the indicators listed in this plan.
   c. Friendly. Describe in general terms the friendly operations or mission and the conditions from which the critical information is derived from. Describe in general terms the friendly vulnerabilities that place the critical information at risk.
   d. Assumptions. List the assumptions that must be made to continue planning.

2. MISSION.
   a. OPSEC Mission Statement.
   b. Critical Information and Indicators. Table 2-1 lists the critical information (CI) associated with XXX. CI is the specific facts about friendly intentions that could be exploited by the adversary, allowing them to plan and act effectively against friendly mission accomplishment. The CI has been assessed to have enough observable indicators or associated friendly vulnerabilities that risk of compromise warrants the development of focused OPSEC measures to protect them. Appendix A aligns this CI with the indicators and resultant OPSEC measures.

<table>
<thead>
<tr>
<th>CI-1</th>
<th>Critical Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI-2</td>
<td>Critical Information</td>
</tr>
<tr>
<td>CI-3</td>
<td>Critical Information</td>
</tr>
</tbody>
</table>

Table 2-1 Critical Information for XXX Operations

c. Vulnerabilities. List the conditions that leave the CI and indicators exploitable by the adversary which has
sufficient knowledge, time, and available resources to thwart friendly mission accomplishment or substantially increase operational risk.

3. EXECUTION.
   a. Concept of Operations. Discuss the details of the operations and how OPSEC is going to support successful mission accomplishment
      (1) Method.
      (2) End State.
   b. Tasks.

4. ADMINISTRATION AND LOGISTICS.
   a. List who is the plan sponsor and costs associated with plan activities at a minimum.

5. COMMAND AND CONTROL.
      (1) Authority.
   b. Command, Control, Communications, and Computer (C4).

6. APPENDICES.
   a. Appendix A: Critical Information, Indicators, and Measures
   b. Appendix B: GLOSSARY
   c. Appendix C: ACRONYMS AND ABBREVIATIONS
APPENDIX A

Critical Information, Indicators, and Measures

**ESSENTIAL SECRET:** Protect the presence, intent, timing, location, and method of XXX Operations

<table>
<thead>
<tr>
<th>Critical Information</th>
<th>Indicator</th>
<th>OPSEC Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI-1: Planning activities are occurring XXX operations.</td>
<td>I-01: List the indicator</td>
<td>O-1: List the OPSEC Measure</td>
</tr>
<tr>
<td></td>
<td>I-02: List the indicator</td>
<td>O-2: OPSEC Measure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>O-3: OPSEC Measure</td>
</tr>
</tbody>
</table>

Table A-1 Critical Information, Indicators and Measures Table

**OPSEC MEASURE DETAILS**

<table>
<thead>
<tr>
<th>WHO</th>
<th>WHAT</th>
<th>WHEN</th>
<th>WHERE</th>
<th>WHY</th>
<th>Check When Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>O-01: OPSEC Measure Details</td>
<td>Who specifically is tasked to execute the measure.</td>
<td>Provide an actionable level of details on the measure.</td>
<td>When will this action take place (date, time, before or after action X).</td>
<td>Where the measure will be executed.</td>
<td>Describes what specifically the measure is achieving- why it is executed the way it is, when it is as well as the conduit or collection means.</td>
</tr>
</tbody>
</table>

Table A-2 OPSEC Measure Details
APPENDIX B
GLOSSARY

APPENDIX C
ACRONYMS AND ABBREVIATIONS
## OPSEC PROGRAM CHECKLIST

### 1. OPSEC Program Manager - per enclosure (3)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Has an OPSEC program manager been designated in writing?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Does the program manager have unimpeded access to the commanding officer?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 Is the program manager a military officer O-3 or above or civilian GS-12 or above with sufficient authority and staff to manage the program?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4 Is the program manager a U.S. citizen?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 Is the program manager a graduate of appropriate OPSEC program manager training?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.6 Does the program manager have a projected rotation date at least 18 months from their date of designation?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7 Is the program manager assigned to the operations department where applicable, or otherwise in a position or department with direct involvement in and information regarding the execution of key command missions, functions and tasks?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.8 Does the program manager possess a minimum of a Secret clearance, and additional clearance and access required to allow unimpeded performance of duties?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.9 Is the program manager not a Public Affairs Officer or member of the public affairs staff?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.10 For two-star and above commands, is the program manager assigned full-time and not as a collateral duty?

2. **OPSEC Working Group – per enclosure (4)**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Does the OPSEC working group include representatives from all key command components, departments, or functions?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 Does the OPSEC working group include representatives from security, anti-terrorism/force protection, intelligence, critical infrastructure protection, public affairs, information assurance, FOIA, and the command technical authority as applicable?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3 Does the OPSEC working group convene at least quarterly?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4 Does the OPSEC working group apply the five-step OPSEC process to the command?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 Does the OPSEC working group recommend appropriate revisions to the CIIL and implementation of OPSEC measures and/or countermeasures?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.6 Are minutes of OPSEC working group meetings recorded and retained?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. **OPSEC Training – per paragraph 5c(3)**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Do command personnel demonstrate awareness of the content of their CIIL, and their specific responsibilities for safeguarding critical information?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Question</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>----</td>
<td>-----</td>
</tr>
<tr>
<td>3.2</td>
<td>Is tailored, command-specific OPSEC training provided to all assigned personnel as part of their onboarding process?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Is OPSEC training required for all personnel prior to granting access to DON networks?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.4</td>
<td>Do all assigned personnel complete OPSEC training at least annually?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>Does command OPSEC training cover the unit CIIL?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>Does command OPSEC training cover social media awareness and vulnerabilities?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7</td>
<td>Does command OPSEC training cover local threats?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.8</td>
<td>Does command OPSEC training cover how to protect, transmit, and destroy controlled unclassified information (such as items on the CIIL)?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.9</td>
<td>Does command OPSEC training cover risks and guidance pertaining to geolocation-capable devices, applications, and services?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.10</td>
<td>Does command OPSEC training cover OPSEC review procedures for public release?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.11</td>
<td>Is command OPSEC training documented?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.12</td>
<td>Does the command conduct family outreach for OPSEC education and awareness?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4. OPSEC Instruction – per enclosure (5)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Does the command instruction contain a CIIL tailored to specific command functions?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td><strong>Is the command CIIL updated as needed and at least annually?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td><strong>Have separate CIILs been considered or implemented for components of the command that are geographically dispersed or have significantly different functions?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td><strong>Does the command instruction provide guidance for the establishment, composition and conduct of an OPSEC working group?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.5</td>
<td><strong>Does the command instruction provide guidance for the conduct of command OPSEC training?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.6</td>
<td><strong>Does the command instruction provide guidance for the reporting and mitigation of disclosures of critical information, and potential disciplinary action against those who violate OPSEC policy?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.7</td>
<td><strong>Does the command instruction provide guidance for approved methods of transmission and disposal of critical information?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.8</td>
<td><strong>Does the command instruction include policy for incorporation of OPSEC into contracts and acquisitions, where applicable?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.9</td>
<td><strong>Does the command instruction include policy for the oversight of the OPSEC programs of subordinate commands, where applicable?</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Other requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Does the command have an approved OPSEC plan (required if conducting sensitive missions, programs and/or operations)? (§5d)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2 Is OPSEC incorporated into the command’s ORM process? (§5e)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.3 Does the command conduct an OPSEC self-assessment at least annually? (§5f)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4 Does the command provide oversight of the OPSEC programs of subordinate commands, and perform an assessment at least every three years? (§5f)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.5 Are command public affairs professionals properly trained in OPSEC concerns and their command CIIL? (§5g)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.6 Do the command public affairs officer and OPSEC program manager work closely with command leadership to coordinate OPSEC and public affairs concerns? (§5g)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ROLES AND RESPONSIBILITIES

1. The SECNAV has overall responsibility for DON OPSEC and its compliance with DoD guidance.

2. The Under Secretary of the Navy (UNSECNAV) is responsible for the oversight, management, readiness, and compliance of DON OPSEC, primarily exercised through the office of the DUSN.

3. The DUSN is designated as the Senior Official in the DON for OPSEC and is delegated responsibility for its oversight, management, readiness, and compliance per references (k) and (l), and advises the UNSECNAV on DON OPSEC issues. DUSN shall:
   a. Develop and promulgate DON OPSEC policy.
   b. Represent the DON on all OPSEC-related, Office of the Secretary of Defense, and inter- and intra-agency working groups, committees, and boards.
   c. Manage all DON OPSEC-related formal tasking and ensure that consolidated DON responses are developed and submitted.
   d. Ensure policies are integrated and coordinated both within the DON and with other services, U.S. Government agencies, allies, and coalition partner programs, operations, and activities as appropriate, per reference (a).
   e. Serve as the DON OPSEC resource advocate.
   f. Provide oversight and periodic assessment of service and DON Secretariat OPSEC programs for compliance with DON and Department of Defense policy.
   g. Coordinate with the services and with the Navy and Marine Corps Inspectors General to provide assessments and oversight of service OPSEC programs.
   h. Provide a representative to the DON Secretariat OPSEC working group.

4. The Department of the Navy Assistant for Administration shall administer, or enter into a memorandum of understanding with another component to administer, the OPSEC program for the DON Secretariat in accordance with the requirements of paragraph 5 of this instruction and lead the DON Secretariat OPSEC working group.

Enclosure (8)
5. All DON Secretariat offices shall designate a representative to the DON Secretariat OPSEC working group.

6. The Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN M&RA) shall ensure that OPSEC awareness training and culture is integrated into individual and unit training programs as required.

7. The Assistant Secretary of the Navy (Research, Development, and Acquisition) (ASN (RD&A)) shall ensure that OPSEC is employed to protect program research, development, testing, and acquisition from potential adversaries. ASN (RD&A) shall:
   
   a. Incorporate OPSEC into program management and acquisition community training at all levels. Specifically, curricula for the acquisition workforce will be reviewed and appropriately updated at their next scheduled refresh to ensure that each acquisition career field receives practical acquisition-focused OPSEC training at each level of certification.

   b. Ensure all contract personnel receive training sufficient to maintain essential secrecy, and at least meeting the requirements of paragraph 5c(3) of this instruction.

   c. Maintain procedures for OPSEC review of contracts for program critical information prior to public release.

   d. Develop procedures to reduce the risk of the release of programmatic and contractual information revealing classified information by aggregation.

   e. Annually review DON SYSCOM programs to ensure compliance with this instruction.

   f. Direct that Program Executive Offices (PEOs) and Direct Reporting Program Managers (DRPMs) comply with this instruction and the OPSEC policies of their host SYSCOM, and are subject to the OPSEC oversight of their host SYSCOM to include review and approval of OPSEC plans for testing and evaluation.

   g. Ensure that PEOs and DRPMs collaborate with their host SYSCOMs in advance of the public release of program information in order to determine potential risks related to public release, and shall maintain a log for program-specific information that is approved for public release, already currently in the public domain, or known to have been compromised.
h. Direct that OPSEC be considered prior to all operational testing and evaluation, with proper authority delegated to suspend testing if an evolution poses an unacceptable risk to relevant critical information.

i. Ensure that as part of the planning for all operational testing and evaluation, PEOs and DRPMs shall affirmatively consider and account for the presence of adversary collection platforms or personnel, to include the presence of treaty-authorized observation aircraft (e.g., aircraft operating pursuant to the Treaty on Open Skies), in the development of OPSEC measures for the specific evolution.

j. Ensure that in addition to adversary collection threats in the physical domain, PEOs and DRPMs shall take into account cyber threats with regard to how and where data containing critical information is transmitted and stored. OPSEC program managers must coordinate with Command Information Officers in developing and implementing local policies that will mitigate OPSEC vulnerabilities.

k. Ensure that PEOs and DRPMs implement tailored OPSEC plans as described in paragraph 5d of this instruction.

l. Appoint in writing an OPSEC program manager to provide oversight over subordinate programs and serve on the DON Secretariat OPSEC working group.

m. Identify acquisition programs with the greatest OPSEC risk and coordinate inspection of OPSEC compliance and effectiveness of those programs with the Naval Inspector General (NAVIG).

8. NAVIG shall coordinate with ASN (RD&A) to inspect and report the OPSEC compliance and effectiveness of DON acquisition programs.

9. The Chief of Information (CHINFO) shall ensure OPSEC considerations are incorporated into all DON public affairs release-of-information processes, guidance, and training per reference (a).

10. The Chief Information Officer (CIO) shall include completion of initial and annual DON OPSEC training as a requirement in the DON Acceptable Use of Information Technology Policy.
11. Director, NCIS shall:

   a. Publish an annual assessment of the foreign intelligence and terrorist threats to the DON that provide OPSEC managers information on adversary priorities, targets, tactics, techniques, procedures, and trends affecting DON interests (references (m) and (n)).

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

12. CNO and CMC shall:

   a. Exercise overall responsibility for their respective service’s OPSEC policy, oversight, resourcing, training, reporting, and implementation of responsibilities.

   b. Issue and maintain an OPSEC instruction and/or order implementing the guidance of this instruction for their respective services, and providing specific guidance regarding organizations and operations.

   c. Establish local guidance implementing OPSEC for their staffs.

   d. Have on staff a full-time OPSEC program manager at a grade of O-4 or GS-13 or higher.

   e. Approve waivers at their discretion to the grade or full-time requirements for OPSEC program managers for commands without a significant operational responsibility that do not engage directly in program or mission support, provided their OPSEC program manager meets all other requirements of enclosure (3).

   f. Impose additional requirements at their discretion for the OPSEC programs of any subordinate commands beyond those of this instruction.

   g. Allocate resources to provide for the required full-time OPSEC program managers at two-star or higher commands without approved waivers.
h. Maintain a service OPSEC support element (e.g., the NOST and MOST) adequately resourced to fulfill their obligations to DUSN and service elements per paragraph 5l of this instruction.

i. Man, train, and equip a cadre of OPSEC planners who are sufficient to meet Combatant Commander and other operational requirements. OPSEC planners shall, at a minimum, be graduates of either the Defense OPSEC Planners Course (DOPC) offered by the Joint OPSEC Support Element, or the Joint Information Operation Planners’ Course (JIOPC) offered by the Joint Forces Staff College. Additionally, ensure that each element that conducts operational planning includes at least one certified OPSEC planner.

j. Direct the establishment of OPSEC working groups at military installations to advise and support installation operations, threat, and force protection working groups per reference (a), and to coordinate OPSEC efforts among tenant commands.

k. In addition to the command OPSEC training requirements described in paragraph 5c(3) of this instruction, direct that tailored OPSEC knowledge and training is incorporated into:

   (1) service accession programs,

   (2) Basic Military Requirements (BMR) portion of rate advancement exams for Sailors and Professional Military Education (PME) requirements for Marines during their next revisions,

   (3) prospective commanding officer, prospective executive officer, mid-career, and other career milestone training, and

   (4) deployment training for personnel and families.

l. Ensure organizational OPSEC lessons learned are captured and disseminated, utilizing the Joint Lessons Learned Information System.

m. Direct the development of mission essential tasks (METs) for OPSEC and incorporate them 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).
n. Direct the development of inspection criteria for OPSEC and ensure that commands have an effective and compliant OPSEC program prior to consideration for operational awards (such as the Navy Battle "E"). Absence of an OPSEC program shall be cause for disqualification.