



DEPARTMENT OF THE NAVY
COMMANDER NAVY RESERVE FORCE
1915 FORRESTAL DRIVE
NORFOLK VA 23551-4615

COMNAVRESFORINST 3070.2
N01S
9 Mar 2021

COMNAVRESFOR INSTRUCTION 3070.2

From: Commander, Navy Reserve Force

Subj: OPERATIONS SECURITY PROGRAM

Ref: See Appendix A

- Encl: (1) Definitions
(2) OPSEC Program Manager Requirements
(3) OPSEC Working Group Requirements
(4) OPSEC Instruction Requirements
(5) Annual OPSEC Posture Assessment Report Format
(6) OPSEC Plan Template
(7) OPSEC Program Checklist
(8) Example of Command Critical Information and Indications List (CIIL)

1. Purpose. Establishes policy, procedures, and responsibilities for the Navy Reserve Operations Security (OPSEC) program per references (a) through (q).
2. Cancellation. COMNAVRESFORINST 3432.1
3. Applicability. The provisions of this instruction are applicable to Navy Reserve personnel (military and civilian) as well as supporting contractor personnel.
4. Policy. Per reference (a), the Navy Reserve Force must maintain an effective OPSEC program to increase operational effectiveness of planned and ongoing U.S. military activities by protecting unclassified indicators which may convey intentions, capabilities or limitations of U.S. Forces. The OPSEC program will ensure coordination between operations, all security disciplines, public affairs, intelligence, training, and command authorities and will include mechanisms for enforcement, accountability, and threat awareness. Programs must establish a balance of protection between sharing of information to the public (including families) and maintaining essential secrecy.
5. Discussion. Commanders must take all OPSEC measures required to prevent disclosure of critical information and maintain essential secrecy.
 - a. 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 information. The maintenance and effectiveness of OPSEC is the responsibility of each commanding officer. Each command must include, at a minimum:

(1) A designated OPSEC program manager meeting the criteria listed in enclosure (3). The program manager must familiarize themselves with the requirements and procedures per references (a) through (f) and any additional guidance from their chain of command.

(2) An effective OPSEC working group per enclosure (3).

(3) The designated OPSEC program manager is responsible for executing a 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 Department of the Navy networks and receive annual training at a minimum. This training must include the unit's CIIL items, 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 and maintained for higher level review as requested. Family outreach must also be performed to educate the families of assigned personnel about OPSEC principles and concerns. Additional guidance on OPSEC family outreach can be found per reference (f).

(4) A local OPSEC instruction per enclosure (4).

b. 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 must be augmented as needed by OPSEC operations plans specific to planned involvement in specific operations.

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

d. Commanders are responsible for oversight, guidance, and supervision over both their OPSEC and that of their subordinate elements. Each command must conduct an annual OPSEC assessment per references (a) and (b), which may consist of either a documented self-assessment, an Inspector General inspection, or a higher headquarters assessment or

9 Mar 2021

assist visit. Additionally, higher level commands must inspect subordinate commands for OPSEC compliance and effectiveness on a tri-annual basis. Assessments must 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.

e. All information considered for release into the public domain must include a review per the appendix to enclosure (3) of reference (g) and must involve an appropriately designated and trained OPSEC professional. All public affairs professionals must be properly trained per references (a) through (c) 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 must work with command leadership to determine when the need for public transparency outweighs the risk of disclosure.

f. OPSEC managers must take into account the wide variety of intelligence collection threats and the exponential growth in the availability of open source information. These trends are likely to continue and must be factored into the development of any OPSEC program. Per reference (p), all Navy Reserve Force commands will ensure all personnel complete Counterintelligence Awareness and Reporting (CIAR) training within 30 days of initial assignment, or employment to their command, and every 12 months thereafter. CIAR training must include the threat from Foreign Intel Entities (FIEs), FIE methods, FIE use of the internet and other communications services, the insider threat, anomalies, reporting foreign travel and foreign contacts, and reporting requirements.

g. Headquarters Industrial Security Specialist and OPSEC program manager must liaison with command contracting officials to ensure OPSEC considerations are included in Performance Work Statements (PWS) of all Navy Reserve Force (NAVRESFOR) contracts. All PWS will receive an OPSEC review at the start and completion of the contracting process to identify critical and/or sensitive information.

h. Critical Information (CI) must 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 CI over an unclassified network is not authorized.

6. Program Reviews and Reporting Requirements. Per reference (a) each command will complete an annual review and evaluation of its OPSEC program and submit a report to their Immediate Superior in Charge (ISIC) OPSEC officer by 30 September of each fiscal year,

reflecting the command's OPSEC posture as of 1 October of that year. Annual assessments must be maintained for a minimum of three years. Enclosure (5) is the annual OPSEC report format and guidance. OPSEC program reviews include:

- a. Command public web assessment for OPSEC indicators, vulnerabilities and risk assessments.
- b. Annual review and validation of OPSEC plans and policies.
- c. OPSEC assessment for evaluation of the command's compliance with OPSEC plans and programs in an effort to appraise its OPSEC posture. The OPSEC assessment may be conducted with a small team of trained personnel from the command's OPSEC working group.
- d. OPSEC surveys conducted to self-evaluate the command's ability to apply the OPSEC methodology to operations. This evaluation should focus on the command's ability to adequately protect CI from adversary intelligence exploitation during command planning, preparation, execution and post execution phases of any command operation or activity.

7. Roles and Responsibilities. Higher level command roles and responsibilities are defined in enclosure (8) of reference (a). Higher level command responsibilities are:

- a. Inspector General must develop and implement a mission applicable OPSEC section for their inspection criteria for assessments of all command's under their cognizance per reference (a) and checklist in enclosure (8).

- b. Commander, Navy Reserve Force N4B and Commander, Naval Air Force Reserve N43 must:

- (1) Per references (a) through (c), ensure the OPSEC process is incorporated throughout the contract acquisition process and when a program's CI or associated indicators are subject to adversary exploitation or unacceptable risk. Ensure and verify that contractors supporting Department of Defense activities use OPSEC to protect Critical Information for specified contracts and subcontracts.

- (2) Determine what OPSEC measures and requirements are essential to protect CI for specific contracts.

- (3) Ensure the Government Contracting Activity identifies those OPSEC measures and requirements in the resulting solicitations and contracts.

- (4) Establish procedures to verify contract requirements properly reflect OPSEC responsibilities and ensure those responsibilities are included in contracts determined to have CI. CI should be determined per references (a) through (c).

9 Mar 2021

(5) Ensure publicly released documents and Statements of Work (SOW) do not reveal CI or CI indicators. If OPSEC planning is necessary in a contract, reflect the OPSEC requirements in the SOW. OPSEC Program Managers should review the SOW prior to public release.

c. Public Affairs must:

(1) Review all information for OPSEC concerns, have the OPSEC manager or officer review as necessary, prior to releasing information to the public.

(2) Ensure unclassified, publicly available websites do not include classified material, Controlled Unclassified Information (CUI), proprietary information, or information that could enable the recipient to infer this type of information.

(3) Periodically remind personnel that all government information must be approved by the PAO for public release prior to posting to any internet site.

(4) Balance the need to publicly release information to garner public support, foster community relations and help with the success of the Navy Reserve with the need to protect CI and CI indicators. The need for OPSEC should not be used as an excuse to deny non-CI to the public.

d. All Hands must:

(1) Be familiar with their command or unit's OPSEC program and procedure through:

(a) Orientation training as a part of the command check-in or command indoctrination program.

(b) Annual training through instructor training, Navy Knowledge Online or computer based training.

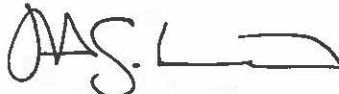
(2) Protect all CI by ensuring they, through their individual or collective actions, do not unintentionally convey indicators of operational intentions, capabilities or limitations.

(3) Ensure CI is not posted to social media. Contact the command OPSEC Officer and/or PAO with any questions regarding the appropriateness of information intended for placement on social media sites. Guidelines and recommendations for using social media technologies in a manner that minimizes risk are located at <https://www.chinfo.navy.mil/socialmedia.html>, and the Chief Information Office Guidelines for Secure Use of Social Media by Federal Departments and Agencies, version 1.0 (<http://www.doncio.navy.mil/Download.aspx?AttachID=11>)

(4) Ensure unclassified, publicly available websites do not display personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers, or e-mail addresses which contain the individual's name. General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable. The names, telephone numbers, and personalized, official e-mail addresses of command or activity public affairs personnel and or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories.

8. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy (SECNAV) Manual 5210.1 of January 2012.

9. Review and Effective Date. Per OPNAVINST 5215.17A, COMNAVRESFOR N01S will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 10 years after effective date unless reissued or cancelled prior to the 10 year anniversary date, or an extension has been granted.



J. A. SCHOMMER
Deputy Commander

Releasability and distribution:

This instruction is cleared for public release and is available electronically only via COMNAVRESFOR Web site, <https://navyreserve.navy.afpims.mil/Resources/Official-Guidance/Instructions/>.

Appendix A

REFERENCES

- (a) SECNAVINST 3070.2A, OPERATIONS SECURITY
- (b) DoDD 5202.02E, DoD Operations Security (OPSEC) Program
- (c) DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual
- (d) CJCSI 3213.01D, Joint Operations Security
- (e) Joint Publication 3-13.3, Operations Security
- (f) NTTP 3-13.3M/MCTP 3-32B, Operations Security (OPSEC)
- (g) DoD Instruction 8550.01, DoD Internet Services and Internet-Based Capabilities of
- (h) DoD Instruction 5230.24, Distribution Statements on Technical Documents
- (i) DoD Instruction 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
- (j) DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- (k) SECNAV M-5214.1, Department of the Navy Information Requirements (Reports) Manual
- (l) SECNAVINST 5500.36, Department of the Navy Security Enterprise of 19 May 2015
- (m) ALNAV 049/13, 171820Z July 2013
- (n) Foreign Intelligence Threat to the Department of the Navy, series, Naval Criminal Investigative Service
- (o) Terrorist Threat to the Department of the Navy, series, Naval Criminal Investigative Service
- (p) DoD Instruction S-3604.01, DoD Military Deception
- (q) DOD Directive 5240.06

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.

b. A U.S. citizen.

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. Must 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 reference (a), enclosure (8), paragraph 12e.

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 service member.

OPSEC WORKING GROUP REQUIREMENTS

1. The working group must 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 must include representatives of all key command components, departments, or functions. Per reference (c), enclosure (a), paragraph 7b(13), it must 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. FOIA
3. Where applicable, it should 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.
4. Minutes must be kept of OPSEC working group meetings and retained for review.

OPSEC INSTRUCTION REQUIREMENTS

1. All commands must 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 three. 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 must 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 enclosure (3).

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

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.

ANNUAL OPSEC POSTURE ASSESSMENT REPORT FORMAT

1. Overview. Summarize the overall OPSEC posture of the command. Highlight strengths and weaknesses that will be addressed in greater detail in the following paragraphs.

a. OPSEC plans and activities conducted during the reporting period. Focus on how the OPSEC process was applied within the command. Avoid emphasizing traditional security measures (e.g., visits to cryptographic materials security custodians, telephone monitoring, procuring secure telephones or improving access control to sensitive areas). Appropriate activities to report include, conducting OPSEC surveys, conducting training about OPSEC and status of establishing command OPSEC programs per references (a) through (d).

b. Miscellaneous problems and recommendations. Address problems not specifically related to matters reported under paragraph a, but which impact the command's OPSEC posture (e.g., designs and operating procedures that hinder effective OPSEC when systems are operated and deficiencies in the OPSEC awareness of personnel before they report to the command). Recommend Chain of Command actions needed to correct problems.

c. Forecast of OPSEC activities and objectives for the next reporting period. Emphasize activities such as those reported in paragraph a.

d. OPSEC Officer. Name, rank, organizational element, Defense Switched Network telephone number and secure telephone number.

e. OPSEC lessons learned. Present concise case studies in the following format (as appropriate, "sanitize" information to allow wide dissemination):

(1) Title

(2) Observation. Concisely state the problem.

(3) Discussion. Answer the "who," "what," "where," "when," "why," and "how" questions about the problem. If the problem could not be solved, explain why?

(4) Lesson learned. State what positive action was taken to avoid or alleviate the problem.

(5) Recommended action. State how to permanently correct the problem or enter "none required".

(6) Comments.

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.

CI-1	Critical Information
CI-2	Critical Information
CI-3	Critical Information

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.

- d. Concept of Operations. Discuss the details of the operations and how OPSEC is going to support successful mission accomplishment.

(1) Method.

Enclosure (6)

(2) End State.

e. Tasks.

3. ADMINISTRATION AND LOGISTICS.

a. List who is the plan sponsor and costs associated with plan activities at a minimum.

4. COMMAND AND CONTROL.

a. Command Relationships.

(1) Authority.

b. Command, Control, Communications, and Computer (C4).

5. 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

Critical Information	Indicator	OPSEC Measure
CI-1: Planning activities are occurring XXX operations.	I-01: List the indicator	O-1: List the OPSEC Measure
	I-02: List the indicator	O-2: OPSEC Measure
		O-3: OPSEC Measure

Table A-1 Critical Information, Indicators and Measures Table OPSEC MEASURE

DETAILS

WHO	WHAT	WHEN	WHERE	WHY	Check When Complete
O-01: OPSEC Measure Details					
Who specifically is tasked to execute the measure.	Provide an actionable level of details on the measure.	When will this action take place (date, time, before or after action X).	Where the measure will be executed.	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.	Admin Purposes.
O-02: OPSEC Measure #2 Details					

Table A-2 OPSEC Measure Details

COMNAVRESFORINST 3070.2
9 Mar 2021

APPENDIX B

GLOSSARY

APPENDIX C

ACRONYMS AND ABBREVIATIONS

Enclosure (6)

9 Mar 2021

OPSEC PROGRAM CHECKLIST

1. OPSEC Program Manager					
	Requirement	Yes	No	N/A	Comment
1.1	Has an OPSEC program manager been designated in writing?				
1.2	Does the program manager have unimpeded access to the commanding officer?				
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?				
1.4	Is the program manager a U.S. citizen?				
1.5	Is the program manager a graduate of appropriate OPSEC program manager training?				
1.6	Does the program manager have a projected rotation date at least 18 months from their date of designation?				
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?				
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?				
1.9	Is the program manager <u>not</u> a Public Affairs Officer or member of the public affairs staff?				
1.10	For two-star and above commands, is the program manager assigned full-time and not as a collateral duty?				

9 Mar 2021

2. OPSEC Working Group					
Requirement		Yes	No	N/A	Comment
2.1	Does the OPSEC working group include representatives from all key command components, departments, or functions?				
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?				
2.3	Does the OPSEC working group convene at least quarterly?				
2.4	Does the OPSEC working group apply the five-step OPSEC process to the command?				
2.5	Does the OPSEC working group recommend appropriate revisions to the CIIL and implementation of OPSEC measures and/or countermeasures?				
2.6	Are minutes of OPSEC working group meetings recorded and retained?				

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

9 Mar 2021

3.12	Does the command conduct family outreach for OPSEC education and awareness?				
4. OPSEC Instruction					
	Requirement	Yes	No	N/A	Comment
4.1	Does the command instruction contain a CIIL tailored to specific command functions?				
4.2	Is the command CIIL updated as needed and at least annually?				
4.3	Have separate CIILs been considered or implemented for components of the command that are geographically dispersed or have significantly different functions?				
4.4	Does the command instruction provide guidance for the establishment, composition and conduct of an OPSEC working group?				
4.5	Does the command instruction provide guidance for the conduct of command OPSEC training?				
4.6	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?				
4.7	Does the command instruction provide guidance for approved methods of transmission and disposal of critical information?				

9 Mar 2021

4.8	Does the command instruction include policy for incorporation of OPSEC into contracts and acquisitions, where applicable?				
4.9	Does the command instruction include policy for the oversight of the OPSEC programs of subordinate commands, where applicable?				

5. Other requirements

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

9 Mar 2021

EXAMPLE OF COMMAND INFORMATION AND INDICATORS LIST

Critical Information List



Critical Information is an adversary's target of choice. Seemingly harmless UNCLAS data combined with other conversations, presentations, e-mails or documents could reveal classified information. Personnel will employ proper Operations Security (OPSEC) and protect Critical Information.

DO NOT DISCUSS CRITICAL INFORMATION OVER UNSECURED TELEPHONE LINES OR UNCLASSIFIED E-MAIL

DO NOT DISCUSS:

*OPERATIONS:

- Status and/or limitations of personnel, equipment, and weapons systems and key contingency concepts processes.
- Standard operating procedures (SOP).
- Specific aspects and changes of Force Protection Conditions.
- Alert status, response times, and schedules.
- Exercise and/or inspection postures and results.
- Mishap and/or accident information of a privileged nature.

*COMMUNICATIONS AND INFRASTRUCTURE:

- Capabilities, configuration, limitations, status, upgrades, or proposed changes related to communication systems, to include networks architecture, transmission systems, relay stations, and associated equipment.
- Specific aspects and changes of Information Operations Conditions.
- Information revealing security measures or weaknesses in communications security or physical security.
- Computer passwords, user IDs, and/or network access paths.
- Security authorization documentation including data provided to support Authorization to Operate or Connect decisions.
- Data collected in order to grant access to DON information technology (e.g., SAAR/Privileged User).
- Lists of critical or executive personnel with mobile devices.

*INTERNET BASED MEDIA:

- Personal Identifying Information.
- Full organizational rosters and telephone directories.
- Contingency plans and/or continuity of operations.
- Building architectural floor plans, diagrams of property or installation.

*PERSONNEL:

- Personnel privacy issues and/or identifiers.
- Identification and relation of command personnel WRT access badges, security eligibility or access.
- Immunization, medical requirements, health status, and deficiencies.
- Location, itineraries, and travel modes of key military and civilian personnel.
- Training deficiencies impairing mission accomplishment.

QUESTIONS? E-MAIL: CNRFC_OPSEC@navy.mil