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

COMNAVRESFORINST 3070.2A
N2
29 Nov 2024

COMNAVRESFOR INSTRUCTION 3070.2A

From: Commander, Navy Reserve Force

Subj: OPERATIONS SECURITY PROGRAM

Ref: (a) NSPM-28
(b) DoDD 5205.02E
(c) DoDM 5205.02
(d) DODD 3115.18
(e) JP 3-13.3 Operations Security
(f) SECNAVINST 3070.2A
(g) ALNAV 072/16
(h) NTTP 3-13.3 Operations Security
(i) JFSC Defense Operations Security Planners Course Handbook (May 2024)
(j) DON OPSEC Program Manager's POAM to execute DUSN (I&S) OPSEC vision
(k) OUSD MEMORANDUM, Guidance on Potential Operations Security Critical Information List Items, 14 OCT 2022
(l) 2022 DoD OPSEC Report—Signed 1 May 2023
(m) COMNAVRESFORINST 5040.1

Encl: (1) Definitions

1. Purpose. Establish policy, procedures, and responsibilities for the Navy Reserve Operations Security (OPSEC) program In Accordance With (IAW) references (a) through (k). The OPSEC program promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. government activities, capabilities, or intentions. The purpose of OPSEC is to identify, control, and protect sensitive unclassified information about a mission, operation, or activity and to deny or mitigate an adversary's ability to compromise that mission, operation, or activity. This instruction has undergone a complete revision and must be reviewed in its entirety.

2. Cancellation. COMNAVRESFORINST 3070.2.

3. Scope. The provision of this instruction applies to all Commander, Navy Reserve Force (COMNAVRESFOR) Echelon II, III, IV, and V commands and all personnel assigned, hereafter collectively referred to as the Reserve Force. This policy applies to all Reserve Force military, Selected Reserve (SELRES), civilians (Reserve Force employees), including contractor employees assigned to Reserve Force commands providing support to activities and operations. All Reserve Force staff are required to read, understand, and comply with this instruction.

4. Definitions. Enclosure (1) list definitions to assist with the implementation of OPSEC.

5. Policy. The Navy Reserve Force must maintain an effective OPSEC program, IAW references (a) through (k), with the capability to identify and protect critical assets, identify and mitigate vulnerabilities, consider foreign intelligence entities' threats in their commands' risk management activities, apply threat mitigation practices to counter the threat, and conduct periodic assessments to continually assess compliance, effectiveness, and risks. 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. The OPSEC cycle will be incorporated into the planning, execution, and assessment of command operations, processes, and activities.

6. Characteristics of OPSEC.

a. Whether the mission is on a battlefield or auditing contracts, effective OPSEC is vital to manage indicators of U.S. intentions, capabilities, operations, and activities.

b. OPSEC shall be considered across the entire spectrum of Department of Defense (DoD) missions, functions, programs, and activities. All DoD personnel, service members, civilians, and contractors must properly safeguard DoD information. OPSEC is everyone's responsibility, and it is critical to the Department's success and the nation's security.

c. OPSEC is (1) an analytic process, (2) focuses on adversary collection capability and intent, (3) emphasizes the value of Critical Information (CI), and (4) is an information related capability.

d. OPSEC methodology operates by a never-ending analytic and objective repetitive process cycle, not a single process.

e. OPSEC capabilities shall include Identity Management principles, including the protection of Personally Identifiable Information (PII), which is a type of CUI.

f. OPSEC shall be integrated with counterintelligence and other security programs, such as those used to address insider threats, CUI, data loss prevention, cybersecurity, Foreign Access Management, physical security, industrial security, and information security.

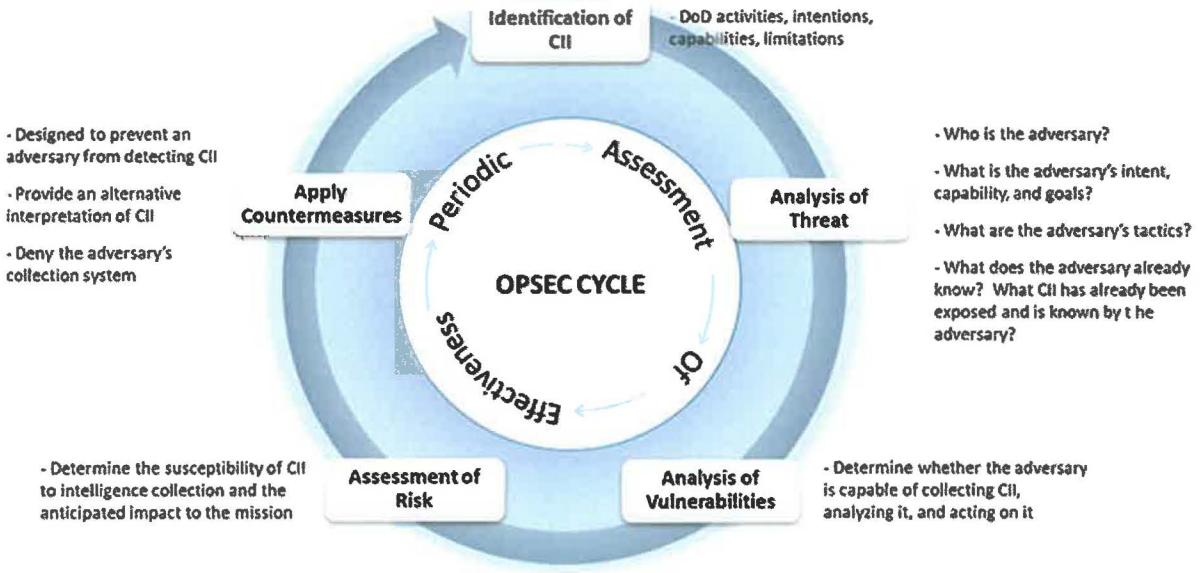
g. To be effective, OPSEC must be a collective effort of various subject matter experts, departments, and activities to fully understand command operations. If involvement in the OPSEC cycle is restricted to a select few representatives, we risk overlooking different perspectives, which are absolute necessary to complete the OPSEC cycle.

h. When working through the OPSEC cycle, it is key to use the adversary's perspective to help identify the CI and indicators, and those vulnerabilities associated with your command, which may be overlooked if we are not using the right mindset.

i. Historically OPSEC was exemplified with reliance on personnel being "tight-lipped" reflected in propaganda posters such as "Loose lips sink ships"; however, this culture fails to appreciate the collection capabilities and methods in the information age. Artificial intelligence, internet of things, surveillance/sensors, and big data are a few of the capabilities and considerations that have changed the paradigm; ordinary, mundane distinct data sets can now be analyzed and combined for context and value to our adversaries. Reserve Force OPSEC grows a culture of educated awareness surrounding the threat posed by ubiquitous data collection, in an information age.

j. Reference (l) identified four high-level findings: (1) Weakness in program establishment and structure; (2) Weakness in OPSEC as a job function; (3) Weakness in program integration; (4) Weakness in training. The report's conclusion was, "inconsistent and insufficient senior leader advocacy for, and a lack of prioritization of, OPSEC programs presents a significant risk of Unauthorized Disclosure (UD) of CI, enables our adversaries and strategic competitors to degrade our operations, puts the safety of our personnel at risk, and impedes our mission success".

k. OPSEC is a continuous cycle that identifies unclassified critical information and indicators (CII), analyzes potential threats and vulnerabilities, assesses risks, and develops countermeasures to safeguard CII. Subsequent sections herein facilitate COMNAVRESFOR OPSEC establishment, structure, roles and responsibilities, integration, and training to operationalize OPSEC awareness, communication, and engagement.



7. Implementation. OPSEC takes into consideration various aspects of the command such as internal and external processes, procedures, governance, risk, threats, vulnerabilities, compliance, assessment, and more. Completing a baseline OPSEC assessment is foundational in defining gaps and shortfalls to establish OPSEC. To facilitate a baseline OPSEC assessment and establish OPSEC; access to guidance, templates, and training aids to implement the OPSEC cycle is necessary.

COMNAVRESFOR, Echelon III and IV OPSEC Program Managers (PMs) and Echelon V OPSEC Coordinators are provided ready access to standardized guidance, templates, and training aids to implement the OPSEC cycle. The COMNAVRESFOR OPSEC PM maintains one MS SharePoint site on Navy Reserve Homeport and two MS TEAMs OPSEC sites, providing OPSEC information tailored to select audiences. Having a central repository ensures real-time posting of and access to current information, supporting OPSEC Working Group (WG) engagement to facilitate active top-down, bottom-up line of communication to support COMNAVRESFOR OPSEC. Echelon III and IV OPSEC PMs are encouraged to develop similar internal MS TEAMs sites to serve as conduits in executing OPSEC to subordinate commands:

a. Commander, Navy Reserve Forces Command (COMNAVRESFORCOM), N2 CI/OPSEC site (Navy Reserve Homeport). Accessible to the Force, but tailored to COMNAVRESFORCOM HQ staff, includes OPSEC overview; policy; COMNAVRESFORCOM OPSEC WG members listing; education; awareness; and tip sheets; to understand, identify, reduce or mitigate OPSEC risks.

b. MS TEAMs COMNAVRESFOR Enterprise OPSEC WG site (PRIVATE MS TEAM site). PRIVATE, access restricted to Echelon III, IV OPSEC PMs (WG members). Enclosures from reference (f) are uploaded and where appropriate, tailored to COMNAVRESFOR use: OPSEC WG Requirements, OPSEC Instruction Requirements, Annual OPSEC Posture Assessment Report Format, OPSEC Plan Template, OPSEC Program Checklist, and Example of Critical Information and Indicators List (CIIL). OPSEC policy, guidance, templates will be developed and refined as necessary to assist in standardizing the implementation of all phases of the OPSEC cycle; generation of designation letters; training documentation; WG minutes; assessments; dashboard/reporting; etc.. Echelon III, IV OPSEC PMs will use provided references and templates, to facilitate OPSEC cycle implementation within their command, and drive command OPSEC culture and policy to subordinate commands.

c. MS TEAMs COMNAVRESFORCOM OPSEC WG site (PRIVATE MS TEAM site). PRIVATE, access restricted to COMNAVRESFORCOM OPSEC PM and internal COMNAVRESFORCOM OPSEC WG members. The COMNAVRESFORCOM OPSEC PM will provide referenced enclosures and templates from the MS TEAMs COMNAVRESFOR Enterprise OPSEC WG site (PRIVATE MS TEAM site) to COMNAVRESFORCOM OPSEC WG members to facilitate OPSEC cycle implementation within their respective department, activity and collectively across the command.

8. Responsibilities.

a. COMNAVRESFOR Chief of Staff (COS) will:

(1) Designate in writing, the COMNAVRESFOR OPSEC PM IAW reference (b), full-time; at grade no lower than O-5 or GS-13, the level necessary to ensure Echelon II authority for the establishment, management, accountability, oversight, and implementation of the COMNAVRESFOR OPSEC Program per references (a) through (m). The COMNAVRESFOR OPSEC PM is assigned full-time to the COMNAVRESFOR/COMNAVRESFORCOM N2 with direct access to Command TRIAD and information regarding the execution of key command missions, functions, and tasks.

(2) Champion and endorse implementation of OPSEC Program horizontally and vertically across the Reserve Force, through the Commanders Intent. Ensure CI and indicators are identified and the risk assessed for each Reserve Force activity related to the planning, development, deployment and movement of equipment, personnel, weapon systems and capabilities and document their mitigation efforts, whether the activity is planned, conducted, or supported.

b. Commanders and Commanding Officers (CO) within the Reserve Force must take all OPSEC measures required to prevent disclosure of critical information and maintain essential secrecy. 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 CI. The maintenance and effectiveness of OPSEC is the responsibility of each CO. Each navy Reserve Activity must include, at a minimum adherence to the following:

(1) Designate an OPSEC PM, Coordinator, or Program Assistant that must familiarize themselves with the requirements and procedures per references (a) through (m) and any additional guidance from their chain of command.

(a) Echelon III and IV Commanders and COs designate in writing, an OPSEC PM meeting the criteria in reference (f) and who will have direct access to the Command TRIAD and report to CO.

(b) Echelon V Commanders and COs designate in writing, an OPSEC Coordinator, at the grade of E6 or above, who will have direct access to all command N-codes, departments, and activities, the Command TRIAD, and report to the CO.

(c) Echelon VI Commanders will designate an OPSEC Program Assistant, who will have direct access to the Reserve Unit TRIAD, the supported command's OPSEC PM or representative, and report to the Reserve Unit CO.

(2) Execute overall responsibility for and support to the command OPSEC PM (Echelon II, III, IV) and Coordinator (Echelon V) in establishment of OPSEC WG per reference (f); local OPSEC Program Plan, command specific OPSEC training program, and command OPSEC policy and guidance.

(3) Provide command guidance for the reporting and mitigation of disclosures of CI and for potential disciplinary action against those who violate OPSEC policies. OPSEC violations should at minimum be documented and reported to the CO, and to higher headquarters upon request.

c. COMNAVRESFOR OPSEC PM. The COMNAVRESFOR OPSEC PM is responsible for Reserve Force OPSEC and COMNAVRESFORCOM OPSEC. The COMNAVRESFOR OPSEC PM will adhere to the following:

(1) Within one year of designation, complete appropriate OPSEC PM 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 IAW reference (f). To augment Navy OPSEC Support Team training, complete Office of the Director of National Intelligence (DNI) National Counterintelligence and Security Center (NCSC) National OPSEC Program OPSE-2380 OPSEC Analysis Course and OPSE-2390 Program Management via MS TEAMs (ETD_REGISTRAR@dni.gov).

(2) Within one year of issuance of this guidance, draft COMNAVRESFORCOM OPSEC Program Plan, describing the implementation of the OPSEC cycle and periodic assessments, and update on an annual basis, prior to 30 September each FY. The OPSEC Program Plan, specific to the local command, will describe the command OPSEC organization, establishment of OPSEC WG, command specific OPSEC training, roles, and responsibilities to conduct all six phases of the OPSEC cycle.

(3) Per DoDD 5240.06, ensure all assigned Reserve Force personnel complete Counterintelligence Awareness and Reporting (CIAR) training within 90 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.

(4) Execute command specific training program that ensures all assigned personnel are aware of the contents of their CIIL and their specific responsibilities for safeguarding CI. 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 (h).

(5) Coordinating across COMNAVRESFORCOM, COMNAVAIRRES, and COMNAVIFORRES; develop, maintain COMNAVRESFOR OPSEC instruction, plan, policies, and procedures to incorporate and institutionalize OPSEC concepts into command mission, functions, and tasks. Review COMNAVRESFOR OPSEC instruction, plan, policies, and procedures annually.

(6) Establish and chair COMNAVRESFOR Enterprise OPSEC WG (Echelon III, IV). At a minimum the OPSEC WG will meet quarterly, document meeting minutes, and support development of the OPSEC Program Plan and OPSEC assessments. The OPSEC WG is charged with ensuring the command and associated family members maintain acute OPSEC awareness through implementation of the OPSEC cycle.

(7) Establish, maintain, and fully implement COMNAVRESFOR OPSEC Strategic Communication Plan to integrate and synchronize lines of communication amongst, both internal and external stakeholders of other information related capabilities, security disciplines and all aspects of COMNAVRESFOR mission, functions, and tasks.

(8) Receive annual OPSEC Assessment Reports from Echelon III and IV command OPSEC PMs by 30 September, each FY.

(9) Conduct Echelon III and IV Command Assessments (CA) to evaluate command OPSEC and Counterintelligence compliance, effectiveness, and risk IAW reference (m).

(10) Establish, maintain, and fully implement COMNAVRESFOR OPSEC Assessment Plan. Continually review, assess, and recommend efficiency and effectiveness aligned to common risk, vulnerabilities, potential threats and mitigation amongst the Reserve Force. Establish requirements for an annual review and assessment of OPSEC cycle procedures (Echelon III, IV) to assist in the improvement of OPSEC Program effectiveness. Review annual OPSEC assessments from Echelon III, IV command OPSEC PMs to determine its effectiveness in the preceding year and to develop recommendations on improvements for the next year and longer term. Maintain a report of these annual reviews, recommendations, and as needed establish internal and external (intra-agency) support and cooperation with respect to Reserve Force OPSEC compliance and effectiveness.

d. COMNAVRESFORCOM OPSEC PM is functionally responsible for administrating OPSEC within their Echelon III, monitoring OPSEC across subordinate Echelon IV, V commands, and will adhere to the following:

(1) Within one year of designation, complete appropriate OPSEC PM 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 IAW reference (f). As an alternative or option to complement Navy OPSEC Support Team training, complete DNI NCSC National OPSEC Program OPSE-2380 OPSEC Analysis Course and OPSE-2390 Program Management via MS TEAMs (ETD_REGISTRAR@dni.gov).

(2) Coordinate and pass guidance to Echelon IV OPSEC PMs.

(3) Within one year of issuance of this guidance, draft COMNAVRESFORCOM OPSEC Plan for implementation of the OPSEC cycle and periodic assessments, and update on an annual basis, prior to 30 September each FY.

(4) Per DoD Directive 5240.06, ensure all assigned COMNAVRESFORCOM 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.

(5) Per reference (f) maintain local COMNAVRESFORCOM OPSEC instruction with policy, process, and procedures to incorporate and institutionalize OPSEC concepts into command mission, functions, and tasks. Please note: Current Immediate Superior in Charge (ISIC) OPSEC instruction can be referenced for local implementation.

(6) Execute command specific training program that ensures all assigned personnel are aware of the contents of their CIIL and their specific responsibilities for safeguarding CI. 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. 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 (h).

(7) Establish, chair COMNAVRESFORCOM OPSEC WG. At a minimum the OPSEC WG will meet quarterly, document meeting minutes, and support development of the OPSEC Program Plan and OPSEC assessments.

(8) Per reference (f) complete annual review and evaluation of command OPSEC program and submit an OPSEC Assessment Report to ISIC OPSEC PM by 30 September of each FY, reflecting the command's OPSEC posture as of 1 Oct of that year. Annual assessments must be maintained for a minimum of three years. Annual OPSEC report format and guidance will be provided by ISIC. Annual OPSEC program reviews include:

(a) Command public web assessment for OPSEC indicators, vulnerabilities and risks.

(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 WG.

(d) OPSEC surveys conducted to self-evaluate the command's ability to apply the OPSEC methodology to command mission, functions, and tasks. This evaluation should focus on the command's ability to adequately protect counterintelligence from adversary intelligence exploitation during command planning, preparation, execution and post execution phases of any command operation or activity.

(9) Per reference (m) support ISIC compliance with COMNAVRESFOR CA Program, specifically with the OPSEC and Counterintelligence program areas.

e. COMNAVAIRFORRES OPSEC PM is functionally responsible for administrating OPSEC within their Echelon III, monitoring OPSEC across subordinate Echelon IV, V commands, and will adhere to the following:

(1) Within one year of designation, complete appropriate OPSEC PM 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 IAW reference (f). As an alternative or option to complement Navy OPSEC Support Team training, complete DNI NCSC National OPSEC Program OPSE-2380 OPSEC Analysis Course and OPSE-2390 Program Management via MS TEAMs (ETD_REGISTRAR@dni.gov).

(2) Coordinate OPSEC with COMNAVRESFOR OPSEC PM and pass guidance to Echelon IV OPSEC PMs.

(3) Within one year of issuance of this guidance, draft COMNAVAIRFORRES OPSEC Plan for implementation of the OPSEC cycle and periodic assessments, and update on an annual basis, prior to 30 September each FY.

(4) Per DoDD 5240.06, ensure all assigned COMNAVAIRFORRES personnel complete 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.

(5) Per reference (f) maintain local COMNAVAIRFORRES OPSEC instruction with policy, process, and procedures to incorporate and institutionalize OPSEC concepts into command mission, functions, and tasks. Please note: Current ISIC OPSEC instruction can be referenced for local implementation..

(6) Execute command specific training program that ensures all assigned personnel are aware of the contents of their CIIL and their specific responsibilities for safeguarding CI. 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. 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 (h).

(7) Establish, chair COMNAVAIRFORRES OPSEC WG. At a minimum the OPSEC WG will meet quarterly, document meeting minutes, and support development of the OPSEC Program Plan and OPSEC assessments.

(8) Per reference (f) complete annual review and evaluation of command OPSEC program and submit an OPSEC Assessment Report to ISIC OPSEC PM by 30 September of each FY, reflecting the command's OPSEC posture as of 1 Oct of that year. Annual assessments must be maintained for a minimum of three years. Annual OPSEC report format and guidance will be provided by ISIC. Annual OPSEC program reviews include:

(a) Command public web assessment for OPSEC indicators, vulnerabilities and risks.

(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 WG.

(d) OPSEC surveys conducted to self-evaluate the command's ability to apply the OPSEC methodology to command mission, functions, and tasks. This evaluation should focus on the command's ability to adequately protect counterintelligence from adversary intelligence exploitation during command planning, preparation, execution and post execution phases of any command operation or activity.

(9) Per reference (m) support ISIC compliance with COMNAVRESFOR CA Program, specifically with the OPSEC and CI program areas. Please Note: COMNAVAIRFORRES may coordinate with COMNAVRESFOR in order to conduct CA on subordinate units. If desired, OPSEC and Counterintelligence program assessments may align with COMNAVRESFOR IG CA schedule or can be assessed at Commander's discretion not to exceed a three-year periodicity.

f. COMNAVIFORRES OPSEC PM is functionally responsible for administrating OPSEC within their Echelon III, monitoring OPSEC across subordinate Echelon IV, V commands, and will adhere to the following:

(1) Within one year of designation, complete appropriate OPSEC PM training offered by a service OPSEC Support Element (e.g., the Navy OPSEC Support Team) or the Interagency OPSEC Support Staff (IOSS), or with a quota to complete training within 90 days of designation IAW reference (f). As an alternative or option to complement Navy OPSEC Support Team training, complete DNI NCSC National OPSEC Program OPSE-2380 OPSEC Analysis Course and OPSE-2390 Program Management via MS TEAMs (ETD_REGISTRAR@dni.gov).

(2) Coordinate OPSEC with COMNAVRESFOR OPSEC PM and pass guidance to Echelon IV OPSEC PMs

(3) Within one year of issuance of this guidance, draft COMNAVIFORRES OPSEC Plan for implementation of the OPSEC cycle and periodic assessments, and update on an annual basis, prior to 30 September each FY.

(4) Per DoD Directive 5240.06, ensure all assigned COMNAVIFORRES 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.

(5) Per reference (f) maintain local COMNAVAIRFORRES OPSEC instruction with policy, process, and procedures to incorporate and institutionalize OPSEC concepts into command mission, functions, and tasks. Please note: Current ISIC OPSEC instruction can be referenced for local implementation.

(6) Execute command specific training program that ensures all assigned personnel are aware of the contents of their 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. 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 (h).

(7) Establish, chair COMNAVIFORRES OPSEC WG. At a minimum the OPSEC WG will meet quarterly, document meeting minutes, and support development of the OPSEC Program Plan and OPSEC assessments.

(8) Per reference (f) complete annual review and evaluation of command OPSEC program and submit an OPSEC Assessment Report to ISIC OPSEC PM by 30 September of each FY, reflecting the command's OPSEC posture as of 1 Oct of that year. Annual assessments must be maintained for a minimum of three years. Annual OPSEC report format and guidance will be provided by ISIC. Annual OPSEC program reviews include:

(a) Command public web assessment for OPSEC indicators, vulnerabilities and risks.

(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 WG.

(d) OPSEC surveys conducted to self-evaluate the command's ability to apply the OPSEC methodology to command mission, functions, and tasks. This evaluation should focus on the command's ability to adequately protect counterintelligence from adversary intelligence exploitation during command planning, preparation, execution and post execution phases of any command operation or activity.

(9) Per reference (m) support ISIC compliance with COMNAVRESFOR CA Program, specifically with the OPSEC and CI program areas. Please Note: Until COMNAVIFORRES has fully operationalized, COMNAVIFORRES may coordinate with COMNAVRESFOR in order to conduct CAs on subordinate units. If desired, OPSEC and CI program assessments may align with COMNAVRESFOR IG CA schedule or can be assessed at Commander's discretion not to exceed a three-year periodicity.

g. Echelon IV OPSEC PM will adhere to the following:

(1) Within one year of designation, complete appropriate OPSEC PM 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 IAW reference (f).

As an alternative or option to complement Navy OPSEC Support Team training, complete DNI NCSC National OPSEC Program OPSE-2380 OPSEC Analysis Course and OPSE-2390 Program Management via MS TEAMs (ETD_REGISTRAR@dni.gov).

(2) Coordinate OPSEC with Echelon III OPSEC PM and pass guidance to Echelon V OPSEC Program Coordinator.

(3) Within one year of issuance of this guidance, draft local command OPSEC Plan for implementation of the OPSEC cycle and periodic assessments, and update on an annual basis, prior to 30 September each FY.

(4) Per DoD Directive 5240.06, ensure all assigned command 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.

(5) Per reference (f) maintain local OPSEC instruction to incorporate and institutionalize OPSEC concepts into command mission, functions, and tasks. Please note: Current ISIC OPSEC instruction can be referenced for local implementation.

(6) Execute command specific training program that ensures all assigned personnel are aware of the contents of their 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. 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 (h).

(7) Per reference (f) complete annual review and evaluation of command OPSEC program and submit an OPSEC Assessment Report to ISIC OPSEC PM by 30 September of each FY, reflecting the command's OPSEC posture as of 1 Oct of that year. Annual assessments must be maintained for a minimum of three years. Annual OPSEC report format and guidance will be provided by ISIC. Annual OPSEC program reviews include:

(a) command public web assessment for OPSEC indicators, vulnerabilities and risks.

(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 WG.

(d) OPSEC surveys conducted to self-evaluate the command's ability to apply the OPSEC methodology to command mission, functions, and tasks. This evaluation should focus on the command's ability to adequately protect counterintelligence from adversary intelligence exploitation during command planning, preparation, execution and post execution phases of any command operation or activity.

(8) Per reference (m) support ISIC compliance with COMNAVRESFOR CA Program, specifically with the OPSEC and CI program areas.

h. Echelon V OPSEC Program Coordinator will adhere to the following:

(1) Within one year of designation, complete DNI NCSC National OPSEC Program OPSE-2380 OPSEC Analysis Course via MS TEAMs (ETD_REGISTRAR@dni.gov).

(2) Per reference (f) maintain local OPSEC instruction to incorporate and institutionalize OPSEC concepts into command mission, functions, and tasks. Please note: Current ISIC OPSEC instruction can be referenced for local implementation. Coordinate OPSEC with Echelon IV OPSEC PM for guidance.

(3) Within one year of issuance of this guidance, draft local command OPSEC Plan for implementation of the OPSEC cycle and periodic assessments, and update on an annual basis, prior to 30 September each FY.

(4) Per DoD Directive 5240.06, ensure all assigned command 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.

(5) Execute local command specific training program that ensures all assigned personnel are aware of the contents of their 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. 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 (h).

(6) Per reference (f) complete annual review and evaluation of command OPSEC program and submit an OPSEC Assessment Report to ISIC OPSEC PM by 30 September of each FY, reflecting the command's OPSEC posture as of 1 Oct of that year. Annual assessments must be maintained for a minimum of three years. Annual OPSEC report format and guidance will be provided by ISIC. Annual OPSEC program reviews include:

(a) Command public web assessment for OPSEC indicators, vulnerabilities and risks.

(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 WG.

(d) OPSEC surveys conducted to self-evaluate the command's ability to apply the OPSEC methodology to command mission, functions, and tasks. This evaluation should focus on the command's ability to adequately protect counterintelligence from adversary intelligence exploitation during command planning, preparation, execution and post execution phases of any command operation or activity.

(7) Per reference (m) support ISIC compliance with COMNAVRESFOR CA Program, specifically with the OPSEC and CI program areas.

(8) Ensure Echelon VI commands have designated an OPSEC representative and have identified their respective supported commands' OPSEC PM.

(9) Ensure Echelon VI commands coordinate with their respective supported commands' OPSEC PM as necessary to ensure Reserve Force OPSEC awareness during supported commands' operations, exercises, or activities.

(10) Track and document annual Echelon VI OPSEC (Uncle Sam's OPSEC, NOST-USOPSEC-3.0) and NCIS Counterintelligence and Insider Threat Awareness and Reporting Training (DON-CIAR-1.0).

i. COMNAVRESFOR N4B and Commander, Naval Air Force Reserve N43 will adhere to the following:

(1) COMNAVRESFOR Industrial Security Specialist and COMNAVRESFOR OPSEC PM 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.

(2) Per reference (h) and in direct coordination with COMNAVRESFOR OPSEC PM, determine and communicate the OPSEC measures required for each contract and ensure they are included in requests for proposal, statements of work, PWSs, statements of operations, or other contract documents.

(3) Per reference (h), COMNAVRESFOR OPSEC PM is responsible for review of contract documents to ensure critical information and indicators are withheld from the public. Provide sufficient detail to ensure complete contractor understanding of the requirements to protect the critical information and/or indicators.

j. Public Affairs will adhere to the following:

(1) In accordance with SECNAVINST 3070.2A, Operations Security, all commands must utilize a process to review information prior to release into the public domain.

Reference (h) includes the operations security (OPSEC) public release form and a decision flow chart as tools or processes to review information for public release. Tailor the form and flow chart to fit the COMNAVRESFOR review requirements.

(2) All public affairs professionals must be properly trained per references (b) through (h) 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 PM must work with command leadership to determine when the need for public transparency outweighs the risk of disclosure.

(3) 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.

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

k. All Hands will adhere to the following:

(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.

(a) 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.

(b) Per reference (f) 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.

9. Assessment. Per reference (m), COMNAVRESFOR Echelon III, IV, and V commands and activities will be assessed on a triennial basis. OPSEC is an assessable program area to ensure mission readiness. CAs, complemented by annual OPSEC Assessments ensures compliance, effectiveness, and risk mitigation IAW references (a) through (k). Each Echelon II, III, IV, V command will adhere to the following:

a. Per reference (f) COMNAVRESFOR IG must develop and implement a mission applicable OPSEC section for their inspection criteria for assessments of all command's under their cognizance.

b. COMNAVRESFOR IG and COMNAVRESFOR OPSEC PM must liaison to review and update as necessary applicable OPSEC and counterintelligence program area questions in reference (m) for clarity and adherence to references (a) through (k).

c. The command OPSEC PM (Echelons III, IV) and OPSEC Coordinator (Echelon V) will comply and support their ISIC in CAs per reference (m) the command OPSEC PM (Echelons II, III, IV) and OPSEC Coordinator (Echelon V) augmented by their respective OPSEC WG members will complete an annual review of their OPSEC Program and submit an OPSEC Assessment to their ISIC OPSEC PM by 30 September of each FY.

d. COMNAVRESFOR OPSEC PM will provide Echelon III and IV OPSEC PMs with access to and guidance to complete Command OPSEC Annual Assessments to assess command and track maturity of their OPSEC program, guide subordinate Echelons in the same.

e. Command OPSEC PMs will provide guidance to subordinate commands as provided by COMNAVRESFOR OPSEC PM to examine effectiveness, both from the adversary's perspective to determine if current procedures protect CI, to identify vulnerabilities; and to implement measures/countermeasures and programmatically against the Interagency OPSEC Support Staff (IOSS) OPSEC Implementation Tiers, to measure maturity of the OPSEC program.

10. 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 OPSEC PM 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. This instruction will be in effect for ten years, unless revised or cancelled in the interim, and will be reissued by the ten-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

M. J. STEFFEN
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/.

DEFINITIONS

1. Controlled Unclassified Information (CUI). Categorical designation that refers to unclassified information that does not meet the standards for national security classification under executive order(s), but is pertinent to the national interest of the United States or to the important interests of entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling, safeguards, or prescribed limits on exchange or dissemination.

2. Counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage or other intelligence activities, such as sabotage, incapacitations, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

3. Critical Indicators. Friendly information, including actions, open-source data, postures, and other perceivable information that an adversary Foreign Intelligence Entity can potentially detect or obtain and interpret to derive friendly Critical Information.

4. Critical Information (CI). Classified or unclassified information important to the achievement of United States objectives and missions that requires safeguarding or dissemination controls and for which unauthorized access to, or modification of, could adversely affect the national interest or national security, the conduct of Federal programs or operations, or individual privacy and Identity Management, and which may be of use to an adversary of the United States.

5. Critical Information and Indicators List (CIIL). A list of critical information and indicators for a specific command or organization.

6. 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.

7. Foreign Intelligence Entity (FIE). Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts activities to acquire sensitive United States information, block or impair United States information, block or impair United States intelligence collection, influence United States policy, or disrupt United States systems or programs. This term includes foreign intelligence services, defined as state intelligence services. This term can also pertain to international terrorists, transnational criminal organizations, foreign cyber actors, or foreign corporations or organizations.

8. Identity Management. OPSEC capability that seeks to mitigate risks to personnel, organizations, missions, and capabilities through the discovery, examination, analysis, assessment, and management of an individual's or organization's identity elements, characteristics, or other attributes in public or non-public records and databases or in social media or other unstructured data sources.

9. Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

10. Information-Related Capability. A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.

11. Operations Security (OPSEC). OPSEC is a capability that identifies and controls critical information and indicators (CII) of friendly force actions attendant to military operations and reduces the risk the adversary can exploit friendly force vulnerabilities by incorporating OPSEC measures and countermeasures. When effectively employed, it denies or mitigates the adversary's ability to compromise or interrupt a mission, operation, or activity. Without a coordinated effort to maintain the essential secrecy of plans and operations, the adversary can forecast, frustrate, or defeat major military operations. OPSEC assists in blinding the adversary, forcing them to make decisions with insufficient information.

12. Operational Aspects. An operational feature, detail, or conclusion that can be derived by adversary collection and analysis of friendly activities. The more operational aspects revealed by observable friendly activities, the greater the value to the adversary as an indicator. Operational aspects used are presence, capability, strength, intent, readiness, location, timing, and method.

13. OPSEC Assessment. An evaluative process of an organization, operation, activity, exercise, or support function to determine if sufficient countermeasures are in place to protect critical information.

14. OPSEC Cycle. Cycle established to support continuous oversight. The OPSEC Cycle phases include: (1) identification of critical information and OPSEC indicators; (2) identification and analysis of relevant threats; (3) analysis of vulnerabilities; (4) assessment of risks; (5) application of appropriate countermeasures; and (6) periodic assessment of effectiveness.

15. OPSEC Posture. The amalgamation of all activities, policies, standards, risk mitigation actions, and processes used to counter adversary exploitation of generally openly available information related to a command's operations or personnel or information that is otherwise critical to mission effectiveness.

16. 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.

17. 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.

18. 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

19. OPSEC PM. An appointee or primary representative assigned to develop and manage an OPSEC program.

20. OPSEC Coordinator. An individual trained in OPSEC who works in coordination with the OPSEC PM.

21. Open Source Research. Monitoring publically available information to identify potential disclosures of critical information and indicators. Open source research does not produce intelligence.

22. Publicly Available Information. Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting a place or attending an event that is open to the public.

23. Risk. A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

24. Risk Assessment. A process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss.

25. Risk Management. The process of identifying, assessing, and controlling risks by making decisions that balance risk costs with mission benefits. Costs may be measured in financial cost, loss of assets, loss of information, or loss of reputation.

26. Threat Analysis. A process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

27. Vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

28. Vulnerability Analysis. A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.