DEPARTMENT OF THE NAVY
OFFICE OF THE JUDGE ADVOCATE GENERAL
1322 PATTERSON AVENUE SE, SUITE 3000
WASHINGTON NAVY YARD DC 20374-5066

JAG/CNLSCINST 3070.2
Code 67
APR 07 2017

JAG/COMNAVLEGSVCCOM INSTRUCTION 3070.2

Subj: OFFICE OF THE JUDGE ADVOCATE GENERAL AND NAVAL LEGAL SERVICE COMMAND OPERATIONS SECURITY PROGRAM

Ref: (a) 06 NOTE 3070 dtd 29 Nov 2016
(b) SECNAVINST 3070.2
(c) OPNAVINST 3432.1

Encl: (1) OJAG/NLSC HQ Critical Information List
(2) OPSEC Program Review Checklist

1. Purpose. This instruction establishes policy for the Operations Security (OPSEC) program for the Office of the Judge Advocate General (OJAG) and Naval Legal Service Command (NLSC), and cancels reference (a). It applies to all military, civilian and contractor personnel employed by, or assigned within, OJAG or NLSC. The OPSEC Program is designed to protect critical information to prevent an adversary from determining friendly intentions or capabilities. It endeavors 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. The OPSEC Program ensures coordination between public affairs, cybersecurity, personnel security, physical security, operations, acquisition, intelligence, training, law enforcement, antiterrorism/force protection, and command authorities, and includes mechanisms for enforcement, accountability, threat awareness, and the highest level of leadership oversight. OJAG and NLSC will incorporate the principles and practice of OPSEC focused on command involvement, planning, assessments, surveys, training, education, threat, resourcing, and awareness.

2. Background. References (b) and (c) establish policy, procedures and responsibilities for the Department of the Navy (DoN) OPSEC program. The following definitions apply:

a. 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.

b. Critical Information List (CIL). A list of critical information that has been fully coordinated within an organization and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

c. Essential Secrecy. The condition achieved from the denial of critical information to adversaries through the combined efforts of traditional security programs and the OPSEC process.

d. Essential Secrets. Aspects of friendly operations that, if compromised, would lead to adversary knowledge of exploitable conditions and a potential failure to meet the Commander's objectives and/or desired end-state.

e. OPSEC Coordinator. An individual trained in OPSEC, located at a subordinate level, who works in coordination with the OPSEC program manager or primary representative.

f. OPSEC Program Manager. A full-time appointee or primary representative assigned to develop and manage an OPSEC program.

3. Responsibilities

a. Assistant Judge Advocate General, Operations and Management (AJAG 06)

(1) Exercise overall responsibility for OPSEC policy, oversight, resourcing, training, reporting and implementation of responsibilities.

(2) Review the Office of the Judge Advocate General (OJAG)/NLSC Headquarters CIL, enclosure (1), at least annually, and approve for publication to all members of OJAG and NLSC.

b. Director, OJAG, Code 67 (Technology, Operations, and Plans)

(1) Serve as the officer primarily responsible for the overall administration of the OPSEC program, and ensure program requirements are met.

(2) Designate, in writing, an OPSEC program manager for OJAG and NLSC headquarters, who must be a U.S. citizen with a favorably-adjudicated single scope background investigation completed within five years prior to assignment and at minimum holds, or is eligible for, a SECRET clearance.

(3) Ensure that the OPSEC program manager for OJAG and NLSC headquarters successfully completes OPSEC practitioner qualification training. As a critical position, it must be filled at all times by a properly trained individual.

(4) Ensure OPSEC is a command emphasis item, and include OPSEC effectiveness as a stand-alone evaluation objective for all operations, exercises and activities.

(5) Ensure annual standardized and division-specific OPSEC training and education are conducted and documented for all Service Members, civilians and contractors, assigned to OJAG and NLSC headquarters starting with orientation programs, and ensure deploying personnel and families receive additional OPSEC training to decrease vulnerabilities and reduce indicators.

(6) Ensure appropriate OPSEC training and accountability documentation is completed for all individuals assigned to OJAG and NLSC headquarters prior to granting access to any DON Nonsecure Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), or other information technology.

(7) Ensure all OJAG and NLSC OPSEC program managers, officers, coordinators, public affairs officers, Freedom of Information Act officers, speechwriters, contracting specialists, Foreign Disclosure Officers and personnel responsible for the review and approval of information intended for public release receive OPSEC training tailored to their duties.

(8) Ensure all OJAG and NLSC OPSEC program managers, officers and/or coordinators are provided the opportunity and resources to attend OPSEC-related courses, conferences and meetings.

(9) Ensure the OJAG/NLSC HQ CIL, enclosure (1), is reviewed, at least annually, and published to all OJAG and NLSC members.

(10) Ensure OPSEC and social media policy is emphasized to the OJAG and NLSC headquarters family readiness support program and incorporated into ombudsman training. This emphasis shall not be limited to periods of deployment or mobilization.

(11) Ensure the review process for public release of information at OJAG and NLSC headquarters includes an OPSEC review to prevent the release of sensitive and/or critical information, which includes information that is determined to be exempt from public disclosure per all applicable laws and regulations.

(12) Resource a capability to conduct and document routine reviews of organization and/or division websites to ensure protection of essential secrets, and to ensure that the content remains relevant, appropriate and devoid of critical and/or sensitive information identified on the CIL.

(13) Ensure an annual self-assessment of OJAG and NLSC headquarters is completed and documented with enclosure (2), and that the results are reported to the OPSEC Program Manager.

(14) Ensure organizational OPSEC lessons learned are captured and disseminated.

(15) Ensure a process is in place to report disclosures of critical information, in order to implement appropriate mitigation measures and execute investigations, as required, to support potential administrative or disciplinary action.

(16) Maintain records of program implementation, review and compliance, including Echelon III command OPSEC instructions, CILs and program review checklists.

(17) Coordinate with all other NLSC commands, as appropriate, to implement this program.

c. NLSC Commanding Officers

(1) Take all OPSEC measures required to prevent disclosure of critical information, to protect essential secrets, and to ensure all personnel understand their responsibilities.

(2) Fulfill all responsibilities outlined in 3.b. above, for their respective NLSC commands. For those duties listed in 3.b. as pertaining only to OJAG or NLSC headquarters, NLSC Commanding Officers shall be responsible for executing the same function at their respective NLSC commands.

(3) Implement a command OPSEC instruction, as required by references (b) and (c), and this instruction, and forward a copy to OJAG, Code 67.

(4) Draft and disseminate to all command members a command CIL, and forward a copy to OJAG, Code 67.

(5) Complete and submit OPSEC program review checklists, as directed by OJAG, Code 67.

(6) Coordinate with all other NLSC personnel, as appropriate, to implement this program.

(7) Ensure personnel are aware that failure to follow OPSEC guidance can result in disciplinary and/or administrative action, and that personnel who violate OPSEC policies will be held accountable.

d. OJAG Division Directors and Special Assistants

(1) Take all OPSEC measures required to prevent disclosure of critical information, including dissemination of the CIL, enclosure (1), to protect essential secrets, and to ensure all personnel understand their responsibilities.

(2) Ensure personnel are aware that failure to follow OPSEC guidance can result in disciplinary and/or administrative action and that personnel who violate OPSEC policies will be held accountable.

e. OPSEC Program Managers

(1) Coordinate and administer the OJAG and NLSC OPSEC program and execute this instruction.

(2) Assist with determination of the command CIL, and disseminate for use by all relevant OJAG and NLSC personnel to identify unclassified information requiring application of OPSEC measures.

(3) Provide command-specific OPSEC orientation and annual awareness training to all command members, as required.

(6) Coordinate with the host installation and other OPSEC program managers located in or on the same facility and/or installation to implement OPSEC awareness, training and assessments.

(7) Conduct and document routine reviews of organization websites to ensure protection of essential secrets, and to ensure that the content remains relevant, appropriate and devoid of critical and/or sensitive information identified on the command CIL.

(8) Conduct and submit self-assessments, using enclosure (2), as directed by OJAG, Code 67.

(9) Capture and disseminate organizational OPSEC lessons learned.

(10) Report disclosures of critical information in order to implement appropriate mitigation measures and required investigations.

(11) Maintain records of program implementation, review and compliance.

(12) Coordinate with all other OJAG and NLSC personnel, as appropriate, to implement this program.

f. Public Affairs Officers

(1) Execute responsibility for the oversight and management of all content on official, publicly-accessible web presences. Ensure OPSEC considerations and CILs are incorporated into all public affairs release-of-information processes, guidance and training, including information released to Congress, budget documents, press releases, speeches, newsletters and official posts to web-based resources.

(2) Conduct and document routine reviews of organization and/or division websites and information releases to ensure protection of essential secrets, and to ensure that the content remains relevant, appropriate and devoid of critical and/or sensitive information identified on the relevant CIL.

(3) Coordinate with all other OJAG and NLSC personnel, as appropriate, to implement this program.

g. Training Officers. Provide support to OJAG Division Directors, OJAG Special Assistants and NLSC Commanding Officers, and coordinate with other OJAG and NLSC personnel, as appropriate, to implement this program.

h. JAG Consolidated Administrative Business Office (JCAB). Review all requirements packages, at the start and at the completion of each contracting process, to identify critical and/or sensitive information, and to ensure that OPSEC measures are a stipulation in all contracts.

4. Records Management. Records created as a result of this notice, regardless of media or format, shall be managed per Secretary of the Navy Manual 5210.1 of January 2012.

h. JAG Consolidated Administrative Business Office (JCAB). Review all requirements packages, at the start and at the completion of each contracting process, to identify critical and/or sensitive information, and to ensure that OPSEC measures are a stipulation in all contracts.

4. Records Management. Records created as a result of this notice, regardless of media or format, shall be managed per Secretary of the Navy Manual 5210.1 of January 2012.

5. Review and Effective Date. OJAG Code 67 will review this instruction annually, on the anniversary of the effective date, to ensure applicability, currency and consistency with federal, DoD, SECNAV, and Navy policy and statutory authority. This instruction will automatically expire 5 years after its effective date, unless reissued or otherwise cancelled prior to the 5-year anniversary date, or an extension has been granted.

JOHN G. HANNINK
Commander, Naval Legal Service Command

J. W. CRAWFORD III
Judge Advocate General

Releasability and distribution:
This notice is cleared for public release and is available electronically via the Office of the Judge Advocate General Web site: http://www.jag.navy.mil

OJAG/NLSC HEADQUARTERS CRITICAL INFORMATION LIST

1. All critical information identified by all host commands and by all supported commands or supported organizations, including Force Protection Conditions.

2. Operational command and control (C2) structure.

3. Sensitive details of current and past cases, client advice, claims and research.

4. Capabilities, configuration, designs, security measures, limitations, status, upgrades or proposed changes related to communication systems and critical infrastructure, to include networks, transmission systems, relay stations and associated equipment.

5. Computer passwords, user IDs and/or network access paths.

6. Security authorization documentation including data provided to support Authorization to Operate or Connect decisions.

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

8. Personal identifying information, including details of command personnel with security clearances or access to special projects.

9. Full organizational rosters and telephone directories.

10. Contingency plans and continuity of operations plans.

11. Architectural or floor plans, or diagrams of buildings.

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

OPSEC Program Review Checklist

Command: _____

Date: _____

Performed by: _____

#	ITEM	YES	NO	N/A
1.	Has the organization appointed, in writing, an OPSEC program manager or coordinator at the appropriate level? (DoDM 5205.02, Enclosure 3.)			
2.	Is the organization OPSEC manager or coordinator someone who is familiar with the operational aspects of the activity, including the supporting intelligence, counterintelligence, and security countermeasures? (SECNAVINST 3070.2, para 4d.)			
3.	Has the OPSEC manager or coordinator completed the appropriate training? (DoDM 5205.02, Enclosure 7.)			
4.	Does the organization have an OPSEC support capability that provides for program development, training, assessments, surveys, and readiness training? (DoDM 5205.02, Enclosure 2.)			
5.	Has the OPSEC manager or coordinator developed local OPSEC guidance (regulations or operating procedures) for use of the OPSEC analytic process? (SECNAVINST 3070.2, para 4c.)			
6.	Has the OPSEC manager or coordinator conducted an annual review and validation of the organization's OPSEC program? (DoDM 5205.02, Enclosure 3.)			
7.	Does the OPSEC manager ensure OPSEC assessments and surveys are conducted? (DoDM 5205.02, Enclosure 4.)			
8.	Does the OPSEC manager or coordinator provide sufficient support for subordinate units he or she has oversight for? (SECNAVINST 3070.2, para 4c.)			
9.	Is the OPSEC manager or coordinator involved in the review process of information intended for public release? (DoDM 5205.02, Enclosure 5.)			
10.	Has the organization ensured that critical information is identified and updated as missions change? (DoDM 5205.02, Enclosure 3.)			
11.	Has the OPSEC manager or coordinator established, implemented, and maintained effective OPSEC education activities to include initial orientation and continuing and refresher training for assigned members? (DoDM 5205.02, Enclosure 7.)			

12.	Does the organization ensure OPSEC is included in activities that prepare, sustain, or employ U.S. Armed Forces during war, crisis, or peace, including research, development, test and evaluation; special access programs; DoD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and release of information to the public, when applicable? (DoDM 5205.02, Enclosure 3.)			
13.	Does the OPSEC manager work with CIP planners to identify critical information related to CIP? (DoDM 5205.02, Enclosure 3.)			
14.	Are assigned personnel aware of the organization's critical information? (DoDM 5205.02, Enclosure 3.)			
15.	Has the component supplemented DoDM 5205.02 and issued procedures for:			
	a. Integrating OPSEC plarming into the plarming, development, and implementation stages of net-centric programs and operating environments? (DoDM 5205.02, Enclosure 2.)			
	b. Conducting OPSEC assessments and surveys? (DoDM 5205.02, Enclosure 4.)			
	c. Handling, safeguarding, and destroying critical information? (DoDM 5205.02, Enclosure 5.)			
	d. A formal review of content for critical information, sensitivity, sensitivity in the aggregate, determination of appropriate audience, and distribution and release controls when releasing information? (DoDM 5205.02, Enclosure 5.)			
	e. Ensuring contract requirements properly reflect OPSEC requirements when appropriate? (DoDM 5205.02, Enclosure 6.)			