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

Canc frp: Nov 2017

06 NOTE 3070
Code 67
NOV 2 9 2016

06 NOTICE 3070

Subj: PHYSICAL SECURITY AND OPERATIONS SECURITY PROGRAMS

Ref: (a) OPNAVINST 5530.14E (Series)
(b) OPNAVINST F3300.53C
(c) NTTP 3-07.2.3
(d) SECNAVINST 3070.2
(e) OPNAVINST 3432.1 (Series)
(f) SECNAV Manual 5510.30

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

1. Purpose. This notice establishes policy for the physical security and operations security programs for the Office of the Judge Advocate General (OJAG) / Naval Legal Service Command headquarters activities in the National Capital Region, encompassing its locations onboard the Washington Navy Yard and the Pentagon. It applies to all military, civilian and contractor personnel employed by, or assigned within, OJAG. These programs have been combined into one notice to properly align responsibilities, functional tasks and awareness to ensure cooperative achievement of programmatic goals.

a. The Physical Security Program is designed to create a secure environment, establish procedures to safeguard personnel, establish controls to prevent unauthorized access to OJAG/Naval Legal Service Command (NLSC) Headquarters facilities and offices, establish effective inventory and controls for equipment, and ensure the safeguarding of documents, electronic files, and information systems against theft, damage, and espionage, in accordance with the references and host installation directives.

b. The Operations Security (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 will incorporate the principles and practice of OPSEC focused on

command involvement, planning, assessments, surveys, training, education, threat, resourcing, and awareness.

2. Background

a. Physical Security. Reference (a) provides guidance and requirements for the Navy's physical security and law enforcement program. Reference (b) establishes the Navy's antiterrorism program, policy, and procedures. Reference (c) provides tactics, techniques and procedures governing the conduct of physical security and law enforcement. While all OJAG personnel are assigned responsibility for the overall physical security of OJAG office spaces, this notice assigns specific responsibilities in order to execute the physical security program.

b. Operations Security. References (d) and (e) establish policy, procedures and responsibilities for the Department of the Navy OPSEC program. The following definitions apply:

(1) Critical Information. Specific facts about friendly intentions, capabilities and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

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

(3) 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.

(4) 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.

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

(6) 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 physical security and OPSEC policy, oversight, resourcing, training, reporting and implementation of responsibilities.

(2) Review the CIL, enclosure (1), at least annually, and approve for publication to all members of OJAG.

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

(1) In execution of the Physical Security Program:

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

(b) Designate a Physical Security Officer in writing and ensure such designated officer is properly certified as a physical security officer.

(c) Designate an Anti-Terrorism /Force Protection (AT/FP) Officer in writing and ensure such designated officer is properly certified as an AT/FP officer.

(d) Maintain and execute Navy AT obligations per reference (a) and conduct an annual assessment of AT program execution and periodic assessments as required.

(e) In coordination with the OJAG Training Officer and the host installation, conduct required annual AT/FP training and maintain records documenting compliance.

(f) Ensure OJAG maintains current Emergency Action Plans (EAP) for all three locations. Designate an OJAG Emergency Management (EM) Officer in writing, and an EM Coordinator for each location to support the EM Officer. Coordinate with the host installation as required for execution of region or installation directives, compliance, and participation in working groups and exercises. Document lessons learned as necessary and report to the host installation.

(g) Ensure implementation of, and compliance with, region and installation FP policies and procedures as directed. Coordinate OJAG plans, responsibilities, and responses with the host installation and inform host installation of OJAG points of contact for FP.

(h) Where mandatory security requirements cannot be met, request appropriate waivers or exemptions.

(i) Coordinate with all other OJAG directorates and Special Assistants, as appropriate, to implement this program.

(2) In execution of the OPSEC Program:

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

(b) Designate, in writing, an OPSEC program manager, 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.

(c) Ensure that the OPSEC program manager successfully completes OPSEC practitioner qualification training.

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

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

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

(g) Ensure all OPSEC program managers, officers, coordinators, PAOs, 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.

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

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

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

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

(l) 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.

(m) Ensure an annual self-assessment is completed, enclosure (2), and that the results are reported to the OPSEC Program Manager of the immediate senior in command.

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

(o) 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.

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

(q) Coordinate with all other OJAG directorates and Special Assistants, as appropriate, to implement this program.

c. Director, OJAG Code 60 (Personnel Support and Program Administration)

(1) In execution of the Physical Security Program:

(a) Manage and execute the Key and Lock Control Program. Designate a Key Control Officer in writing.

(b) Ensure proper personnel access to facilities and spaces, to include restricted areas, and maintain required records and documentation to ensure individual accountability. Ensure key distribution, access, and tracking is performed as part of command check-in and check-out procedures.

(c) Ensure execution of, and compliance with, personnel security clearance and access procedures, and maintain required documentation in accordance with reference (f).

(d) Ensure the certification and physical integrity of restricted spaces (including sensitive compartmented information facilities) and open container areas under the control of OJAG, and maintain compliance and required documentation. Conduct inspections, at least annually and periodically as required, of restricted areas and open container areas to ensure compliance with reference (b). Coordinate as required with the host installation.

(e) Where mandatory security requirements cannot be met, request appropriate waivers or exemptions.

(f) Where violations of authorities, procedures, or requirements have been committed, report criminal activity and significant incidents to designated authorities and initiate command investigations as appropriate.

(g) Inform host installation commanders/commanding officers of all areas under OJAG control designated as restricted areas.

d. OJAG Division Directors and Special Assistants

(1) In execution of the Physical Security Program:

(a) Within their respective staff and headquarters activities, execute required daily and/or periodic physical checks of facilities, spaces, restricted areas, containers, information systems, and ingress/egress points to ensure facility physical integrity and security standards, and maintain required records and documentation of such checks.

(b) Within their respective staff and headquarters activities, ensure implementation of security directives and measures and training compliance, as coordinated by OJAG Codes 60 and 67.

(2) In execution of the OPSEC Program:

(a) 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.

(b) Ensure personnel are aware that failure to follow OPSEC guidance can result in disciplinary and/or administrative action.

(c) Report all incidents of Classified Data and/or PII spillage immediately to the ISSO or ISSM or their Command designee as soon as the incident is known.

e. Public Affairs Officer. In execution of the OPSEC Program:

(1) Execute responsibility for the oversight and management of all content on official, publicly-accessible web presences. Ensure OPSEC considerations and the CIL are incorporated into all OJAG 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 CIL.

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

f. OPSEC Program Manager

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

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

(3) Provide OPSEC orientation and annual awareness training to all personnel, as required.

(4) Ensure and verify that contractors supporting OJAG activities use OPSEC to protect critical information for specified contracts and subcontracts.

(5) Lead OPSEC working group meetings, as required, consisting of at least one representative from each division.

(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 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.

(8) Conduct self-assessments and surveys at least annually, enclosure (2), and report the results to the OPSEC Program Manager of the immediate senior in command.

(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 personnel, as appropriate, to implement this program.

g. Physical Security Officer

(1) Coordinate and administer the Physical Security program and execute this instruction.

(2) Coordinate with the host installation and other physical security officers located in or on the same facility and/or installation to implement physical security programs.

(3) Implement installation force protection policies and procedures, as directed, and coordinate plans, responsibilities and responses with the installation.

(4) Actively participate in installation antiterrorism, law enforcement, and emergency management exercises, from initial planning through the exercise to documentation of lessons learned.

(5) Establish a system for the daily after-hours checks of restricted areas, facilities and containers to detect any deficiencies or violations of security standards.

(6) Provide physical security orientation and refresher training to all personnel, as required. Security education programs shall include, but are not limited to, general security safety and awareness, theft prevention, and installation-specific security procedures.

(7) Conduct self-assessments at least annually, and report the results to the Director, OJAG, Code 67.

(8) Report all physical security incidents, violations, vulnerabilities and deficiencies to Director, OJAG, Code 67, in order to implement appropriate mitigation measures and required investigations.

(9) Where mandatory security requirements cannot be met, request appropriate waivers or exemptions.

(10) Maintain records of program implementation, review and compliance. Maintain records of security violations for a period of 3 years.

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

h. Training Officer. Provide support to the Directors of Codes 60 and 67, and coordinate with other OJAG directorates and special assistants, as appropriate, to implement this program.

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

5. Cancellation. This notice will remain in effect for one year unless superseded by subsequent notice.

G. E. SHARP
Assistant Judge Advocate General
(Operations & Management)

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 CRITICAL INFORMATION LIST

1. OPERATIONS

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

b. Operational command and control (C2) structure.

c. Standard operating procedure (SOP).

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

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

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

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

h. Alert status, response times and schedules.

i. Exercise and/or inspection postures and results.

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

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

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

m. Military Information Support Operations.

n. Military Deception Plans and Operations.

o. Results of adversary operations or battle damage against U.S. forces that could provide measures of effectiveness to the enemy.

2. PLANS

a. Changes in wartime mission and/or tasking.

b. Specific information of schedule of forces, equipment or staging locations.

c. Security classification of a classified operation, program or project.

d. Intent to mobilize before public announcement.

e. Infrastructure reports.

f. Evacuation routes, procedures and rally points.

g. Intended operational changes before public announcement.

3. COMMUNICATIONS AND INFRASTRUCTURE

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

b. Technical system architectures, capabilities, vulnerability information and security assessment reports related to C2 systems or National Security Systems.

c. Security, network architecture, topology, infrastructure, infrastructure design and security risk assessment results of DON information technology.

d. Location, schematics, capabilities, protection measures, vulnerabilities and degradation of critical infrastructure.

e. Network architecture diagrams or documents.

f. Information revealing a communications security weakness or physical security weaknesses.

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

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

i. Data collected in order to grant access to DON information technology, e.g., System Authorization Access Request forms.

4. INTELLIGENCE

a. Intelligence sources or methods of gaining intelligence; analytical methods and processes.

b. Intelligence assessments, maps and locations of intelligence targets.

c. Intelligence, surveillance and reconnaissance resources.

d. Counterintelligence capabilities.

e. Intelligence gaps and limitations.

5. LOGISTICS

a. Changes or shortages in equipment and/or command status that may impair mission capabilities.

b. New equipment capabilities and/or limitations.

c. Logistical posture of U.S. and allied forces.

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

7. INTERNET BASED MEDIA

a. Personal Identifying Information.

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

c. Full organizational rosters and telephone directories.

d. Contingency plans and/or continuity of operations.

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

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

8. PERSONNEL

a. Personnel privacy issues and/or identifiers.

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

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

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

e. Manpower gains or losses associated with contingency operations or

exercise.

f. Training deficiencies impairing mission accomplishment.

g. Lists of personnel in the DON Cybersecurity workforce.

h. Lists of critical or executive personnel with mobile devices.

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 planning into the planning, 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.)			