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

JAG/CNLSCINST 5239.3
Code 67
NOV 18 2016

JAG/COMNAVLEGSVCCOM INSTRUCTION 5239.3

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

Ref: (a) SECNAVINST 5239.3C
(b) SECNAV M-5239.2
(c) DON CIO Memorandum, "Acceptable Use of Department of the Navy (DON) Information Technology," February 12, 2016
(d) SECNAV M-5510.36
(e) COMNAVNETWARCOM 300305Z Nov 10, CTO 10-25
(f) COMNAVNETWARCOM 012255Z Dec 10, CTO 10-25A

Encl: (1) Cybersecurity Program

1. Purpose

a. To ensure compliance with standards for Cybersecurity (CS), information systems resources and operations, Cybersecurity workforce development, Cybersecurity training under Department of Defense Information Networks – Navy (DODIN-N) and Defense Information Systems Network (DISA) requirements.

b. To establish a Cybersecurity program to implement references (a) through (f) within the Office of the Judge Advocate General (OJAG) and Naval Legal Service Command (NLSC) to protect and safeguard Navy Information Cyberspace, computer equipment and network systems in support of Defense-in-Depth across the Global Information Grid (GIG).

c. To identify the principal roles and responsibilities for managing and executing the NLSC Cybersecurity policy, including duties of key Cybersecurity Workforce personnel, commanding officers and all personnel.

d. To direct NLSC Information Technology (IT), Cyberspace, and information system planning and architecture at all stages from accreditation through life-cycle management to ensure compliance and alignment with DODIN-N principles and Department of the Navy (DON) Security-in-Depth, Cybersecurity strategies and the Risk Management Framework (RMF).

2. Cancellation. COMNAVLEGSVCCOMINST 5239.2.

3. Scope

a. This instruction applies to OJAG and all NLSC activities, organizations, contractors, personnel, and information systems including, but not limited to:

(1) Information systems and networks used to enter, receive, process, store, display or transmit unclassified, sensitive, or classified information;

(2) Information systems and networks used to support NLSC systems that process data or information; and,

(3) Information systems and networks procured, developed, modified, operated, maintained, or managed by or on behalf of NLSC.

b. This instruction addresses adherence to operations principles as set forth by Operations, U.S. Fleet Cyber Command (FCC), Naval Network Warfare Command (NETWARCOM), and Department of Defense Information Networks – Navy (DODIN-N) principles as subsets of the overall NLSC Cybersecurity (CS) policy.

4. Policy. All NLSC commands, activities, Cybersecurity Workforce members, and personnel shall implement Cybersecurity program requirements contained in both this instruction and references (a) through (f). Policies and requirements set forth by higher authority shall take precedence over the policy established in this instruction in any cases of conflict, except where a security requirement set forth in this requirement is more restrictive than those set forth in higher directives.

5. Responsibilities

a. Assistant Judge Advocate General, Operations and Management (AJAG 06). Serve as the NLSC Local Cybersecurity Authority (LCSA), and appoints the NLSC Command Information Officer (CIO) and the NLSC Command Information Systems Security Manager (ISSM) in writing.

b. NLSC Command Information Officer (CIO). Report to the NLSC LCSA and has delegated responsibility to:

(1) Ensure compliance with DoD and DON Cybersecurity policy to ensure complete Cybersecurity Readiness within the NLSC organizations.

(2) Establish NLSC Cybersecurity Policy and Procedures.

(3) Oversee ISSM and ISSO Cybersecurity functions and management of the Cybersecurity Program.

(4) Designate the NLSC ISSM in writing.

(5) Oversee and manage organization Cybersecurity (CS) training programs, implement oversight procedures to ensure core CS/IAWF training, certification, education, and management requirements are met and consistent per reference (b) with DON oversight and service direction.

(6) Ensure NLSC Commands are physically inspected by the ISSM, ISSO or Command ISSO at least once per year, with Article 6 inspections. ISSO's shall validate Cybersecurity (CS) policy implementation through formalized Cybersecurity checklists, through both onsite and remote assessments.

(7) Mitigate the adverse effects of unauthorized access to unclassified/classified systems and information by investigating and acting upon reports of security violations and compromises of unclassified/classified information and systems.

c. NLSC Information Systems Security Manager (ISSM). Report to the NLSC CIO, and will:

(1) Complete and report annual Cybersecurity Training Continuing Education Hours (CEH) commensurate with commercial certification requirements and reference (b). Maintain certification requirements and provide course completion certificates to the NLSC CIO in digital format. Training length and requirements shall be commensurate with current commercial certification issuer and guidelines in reference (b).

(2) Ensure compliance with DoD and DON Cybersecurity policy to ensure complete Cybersecurity Readiness within the NLSC Commands.

(3) Establish NLSC Cybersecurity policy and procedures.

(4) Perform routine risk assessments and inspections of NLSC information systems and Cybersecurity programs.

(5) Ensure compliance with accreditation and certification standards, as well as timely and successful approval of requests to Department of the Navy Assistant for Administration (DON/AA) for Authority to Operate (ATO) and Interim ATO (IATO) NLSC Cybersecurity systems, software or programs.

(6) Oversee the Cybersecurity Workforce, qualifications and compliance per reference (b).

(7) Oversee Cybersecurity functions and management of the Cybersecurity Program.

(8) Designates NLSC ISSOs in writing.

(9) Implement the NLSC Cybersecurity Program consistent with Local Cybersecurity Authority duties identified above and in accordance with current DoD and DON Cybersecurity policy.

(10) Develop IT Security Plans of Action and Milestones (POA&Ms) in accordance with reference (a) to delineate and schedule tasks necessary to resolve identified Cybersecurity and program weaknesses. Prioritize and monitor the progress of the mitigation of identified weaknesses to acceptable levels of risk.

(11) Mitigate the adverse effects of unauthorized access to unclassified/classified systems and information by investigating and acting upon reports of security violations and compromises of unclassified/classified information and systems.

(12) Request vulnerability assessment assistance as required.

d. NLSC Information Systems Security Officers (ISSO). Report to the NLSC ISSM, and will:

(1) Complete and report annual CEH commensurate with commercial certification requirements and reference (b). Maintain certification requirements and provide course completion certificates to the NLSC ISSM in digital format. Training length and requirements shall be commensurate with current commercial certification issuer and guidelines in reference (b).

(2) Assist the ISSM in ensuring compliance with DoD and DON Cybersecurity policy to ensure complete Cybersecurity Readiness within all OJAG/NLSC Commands.

(3) Assist the ISSM in performing routine risk assessments of NLSC information systems and Cybersecurity programs.

(4) Assist the ISSM and CIO in establishing NLSC Cybersecurity policy and procedures.

(5) Assist the ISSM in ensuring compliance with accreditation and certification standards, as well as timely and successful approval of requests to DON/AA for ATO and IATO NLSC Cybersecurity systems, software or programs.

(6) Assist the ISSM in implementing the NLSC Cybersecurity Program consistent with Local Cybersecurity Authority duties identified above and in accordance with DoD and DON Cybersecurity policy.

(7) Approve System Authorization Access Request-Navy (SAAR-N) and verify certificates required for network access.

(8) Ensure all software updates and security patches on standalone computers and devices have been implemented on a monthly basis or more often as needed to combat zero-day cyber threats or based on direction provided by DISA and DON-CIO.

(9) Maintain inventory of all non-disposable IT assets and ensure standalone computer assets do not exceed a four-year life-cycle in compliance with DoD mandates.

(10) Ensure Cybersecurity compliance with all DoD, DON-CIO and Naval Network Warfare Command (NETWARCOM) guidance.

(11) Ensure all IT assets are disposed of and destroyed properly in coordination with OJAG/NLSC, DON and NSA Center for Storage Device Sanitization Research guidelines for unclassified and classified data/media destruction.

(12) Mitigate the adverse effects of unauthorized access to unclassified/classified systems and information by investigating and acting upon reports of security violations and compromises of unclassified/classified information and systems.

e. Command Administrative Officers (AO).

(1) Identify security deficiencies at their commands and branches and take appropriate corrective action to correct the deficiencies to achieve an acceptable level of risk.

(2) Ensure all safeguards and countermeasures (e.g., port security, host-based network scanning and intrusion detection/prevention devices) required to maintain an acceptable level of risk are implemented and maintained.

(3) Ensure a continuing risk management process is in effect to minimize the potential for unauthorized disclosure of sensitive information, modification or destruction of assets, or denial of service.

(4) Ensure process/data ownership is established and maintained for each information system, to include accountability, access rights, and special handling requirements.

(5) Ensure IT Cybersecurity, information and network security protocols meet current DoD and DON standards while also enabling the most efficient performance of authorized tasks and system access.

(6) Ensure users receive access only to the information, resources and systems necessary on a "need to know basis" for the performance of assigned functions to which they are authorized by virtue of their billet, position, contract and appropriate security clearance for position held.

(7) Consider information system security policies throughout the life cycle of all information technology from concept development through design, development, deployment, acquisition, operation and maintenance until replacement or disposal.

(8) Ensure that Cybersecurity awareness, training, education, and Cybersecurity certification are verified compliant for all military, civilian and contractor personnel annually.

(9) Maintain System Authorization Access Request-Navy (SAAR-N) forms and training certifications for each command member either in electronic or paper format, with electronic format as the preferred method.

(10) Mitigate the adverse effects of unauthorized access to unclassified/classified systems and information by investigating and acting upon reports of security violations and compromises of unclassified/classified information and systems. All such incidents must be reported to the NLSC Lead ISSO or ISSM immediately upon discovery.

f. Director, OJAG Code 67. Serve as the NLSC Removable Media Representative (RMR), report to the LCSA per references (e) and (f). Also, will:

(1) Designate command Data Transfer Agents (DTA) in writing.

(2) Provide guidance required to transfer classified data via removable media on the Standard Internet Protocol Router Network (SIPRNet) workstations and servers that have been previously approved by designated OJAG/NLSC commands.

(3) Provide copies of written authorization to the ISSM or ISSO for each approved DTA to include full name, rank/grade, and Electronic Data Interchange-Personal Identifier (EDIPI).

(4) Provide make, model, serial number and location of each computer system approved for removable media to the ISSM or ISSO.

(5) Establish quarterly RMR reporting requirements per references (e) and (f).

(6) Mitigate the adverse effects of unauthorized access to classified systems and information by investigating and acting upon reports of security violations and compromises of classified information and systems.

g. Division Directors, Special Assistants, and NLSC Commanding Officers.

(1) Designate, at a minimum, two personnel who are in charge of submitting SAARs for user accounts utilizing the SAAR workflow in SharePoint.

(2) Recommend to the RMR, for those commands requiring access to SIPRNET resources, two military or civilian personnel to be designated as command DTAs.

(3) Ensure all members complete annual Cybersecurity awareness training.

(4) Create an organizational culture that embraces and promotes the importance of Cybersecurity.

h. NLSC Users.

(1) Report all incidents of classified data and personally identifiable information spillage immediately to their AO/Command Security Officer (CSO), ISSM or ISSO.

(2) Complete Cybersecurity awareness training annually and provide their training certificate to their AO.

5. Action

a. All NLSC commands, activities and personnel shall comply with this NLSC Cybersecurity Program, and with DoD and DON Cybersecurity programs and policies.

b. The NLSC CIO will inspect compliance to this Cybersecurity Program by detailing the ISSO as a member of the NLSC Inspector General Article 6 Inspection team, or through independent ISSO visits to NLSC commands between Article 6 Inspection cycles.

6. 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.

7. 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, using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after its effective date, unless reissued or otherwise canceled prior to the 5-year anniversary date, or an extension has been granted.

G. E. SHARP
Assistant Judge Advocate General for
Operations and Management
Chief of Staff, Region Legal Service Offices,
Naval Legal Service Command

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the JAG Website, http://www.jag.navy.mil.

Cybersecurity Program

1. NLSC Cybersecurity Program Compliance and Reporting

a. The NLSC ISSM and ISSOs are responsible for executing and monitoring the Cybersecurity Program throughout the NLSC enterprise.

b. The NLSC ISSM and ISSOs are responsible for reporting Cybersecurity status and/or compliance via approved incident reporting and inspection systems, and via the reporting chain of command.

c. OJAG/NLSC personnel will report all incidents of classified and PII spillage to the ISSM or ISSO or their designee within 24 hours of the incident or per reference (d).

d. NLSC commands that require the issuance of SIPR Tokens for their personnel must establish a minimum of two Trusted Agents (TA) for the National Security System (NSS) Public Key Infrastructure (PKI) Program, to issue SIPR Tokens as needed to comply with mission critical data sharing protocols.

(1) Command TA's must complete the TA training located at https://infosec.navy.mil/PKI/tatraining.html.

(2) Command TA's utilizing the Card Issuance Workstation (CIW) software pushed from the Navy Marine Corps Intranet (NMCI) or DVD installation and may receive a batch of blank tokens, Certificate Registration Instructions (CRIs) for their registered users. The TA will utilize the CIW software to complete enrollment of the user token.

(3) Each OJAG and NLSC command will gather and forward subscriber registration information to the Registration Authority (RA)/Local Registration Authority (LRA).

e. Reportable Cybersecurity program information includes, but is not limited to cybersecurity annual training completion, cybersecurity incident reporting, copyright violations and unauthorized software use, and information security violations.

2. Information Technology (IT) System Development

a. The NLSC CIO, ISSM, and ISSO will implement and maintain an adequate level of security-in-depth posture for all information technology resources (i.e., Information Systems (IS), applications, networks) under their cognizance.

b. Early and continuous involvement of the NLSC CIO and Cybersecurity workforce, users, security staff, and process owners is required when defining and implementing security requirements for IT systems, information systems, software and networks.

c. All purchases of IT products shall be pre-approved by the NLSC CIO in the Navy Information Technology Approval System (NAV-ITAS) to ensure compliance with existing DON standards except as noted below:

(1) Storage media. All storage media must comply with security regulations regarding handling, marking/classification, storage, safeguarding and destruction, with these additional provisions:

(a) CD-R and DVD-R disks may be procured without NLSC CIO pre-approval.

(b) External hard drives must be approved for purchase by ISSM or ISSO.

(2) Computers and IT devices. All computer purchases, other than NMCI assets, must be received and inventoried at OJAG Code 67 for initial load of baseline software such as Operating System, Antivirus Software and other mission critical applications. Operating systems and the standard suite of applications for non-NMCI computer and information system assets will be updated with security patches by OJAG Code 67 or designated and authorized Administrative personnel. Updates and security patches will be performed only by the following methods:

(a) Shipping to Code 67 for update;

(b) Software update by DVDs issued by Code 67;

(c) Secure VPN update push; and

(d) Local Wi-Fi updates.

(3) Software.

(a) All software purchases must be approved by Code 67 and entered into NAV-ITAS and approved for use in DON Applications and Database Management System (DADMS).

(b) Copyright Policy (use of proprietary software). Proprietary software shall be used in a manner consistent with the manufacturer's license agreement. The U.S. Government is not exempt from copyright infringement liability. If an employee violates copyright law or other conditions of a software licensing agreement, disciplinary action may be taken. Employees who violate NLSC policy on copyright issues or whom direct others to violate that policy are not considered to be acting in their official capacity and may be held personally liable for civil damages resulting from copyright infringement. SECNAVINST 5870.4A addresses permission to copy materials subject to copyright. All violations of license agreement materials must be reported to the NLSC CIO, ISSM, ISSO or CISSO.

3. <u>Information Security</u>

a. When processing classified information, activities must comply with DoD and DON Information Security Program and Cybersecurity policies and instructions.

b. Additional guidance for NLSC Information Security programs and procedures is contained in reference (g).

c. Labeling of data stored on magnetic media is required in controlled access areas (areas which handle/process classified data/information) and shall be in accordance with GSA, Information Security Oversight Office (ISOO) guidelines utilizing the following standard forms (labels):

Form Number	Title	Stock Number
SF 706	TOP SECRET label	SF 706:7540-01-207-5536
SF 707	SECRET label	SF 707:7540-01-207-5537
SF 708	CONFIDENTIAL label	SF 708:7540-01-207-5538
SF 709	CLASSIFIED label	SF 709:7540-01-207-5540
SF 710	UNCLASSIFIED label	SF 706:7540-01-207-5539
SF 711	Data Descriptor label	SF 706:7540-01-207-5541

These labels may be ordered from GSA using FEDSTRIP/MILSTRIP procedures. The SF 709, CLASSIFIED label, shall only be used when the output is classified but the level of classification has not yet been determined. UNCLASSIFIED labels shall be utilized in any environment where classified information of any level is stored or processed in the same area as unclassified data.

4. Operations and Network Security. In all electronic and other communications, all personnel must comply with DoD, DON and NLSC programs regarding Operations Security (OPSEC) and Network Security (COMSEC) in order to safeguard mission readiness and safety of operations, and to ensure the proper use of DoD/DON networks, information systems and communication systems.