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

IN REPLY REFER TO

JAG/COMNAVLEGSVCCOMINST 5239.2
Code 65
03 DEC 2010

JAG/COMNAVLEGSVCCOM INSTRUCTION 5239.2

From: Judge Advocate General
Commander, Naval Legal Service Command

Subj: INFORMATION ASSURANCE PROGRAM

Ref: (a) DOD Directive 8500.01E
(b) SECNAVINST 5239.3B
(c) OPNAVINST 5239.1C

Encl: (1) Information Assurance Program Policy
(2) Definitions

1. Purpose

b. To ensure compliance with standards for information assurance (IA), information systems resourcing and operations, IA workforce development, and IA training under Department of Defense (DoD) and Department of the Navy (DON) requirements.

a. To establish an IA program to implement references (a) through (c) within the Office of the Judge Advocate General (OJAG) and Naval Legal Service Command (NLSC) to protect and safeguard Navy information and network systems in support of defense-in-depth across the Global Information Grid (GIG).

2. Cancellation. This instruction supersedes and cancels JAGINST 5239.1 and COMNAVLEGSVCCOMINST 5239.1A.

3. Scope.

a. This instruction applies to all OJAG and 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 OJAG and NLSC systems that process data or information; and,

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

b. This instruction addresses adherence to Operations Security (OPSEC), Communications Security (COMSEC) and Information Security (INFOSEC) principles as subsets of the overall OJAG/NLSC IA policy.

4. Definitions. See Enclosure (2).

5. Objectives

a. To implement IA policy and procedures within OJAG and the NLSC organizations to comply with DoD and DON IA Programs;

b. To identify the principal roles and responsibilities for managing and executing the OJAG/NLSC IA policy, including duties of key IA Workforce personnel, commanding officers and all personnel;

c. To direct OJAG/NLSC IT and information system planning and development at all stages from accreditation through life-cycle management to ensure compliance and alignment with DoD and DON Defense-in-Depth and Defense-in-Breadth IA strategies.

6. Policy. All OJAG/NLSC commands, activities, IA Workforce members, and personnel shall implement IA program requirements contained in both this instruction and references (a) through (c). Policies and requirements set forth by higher authority shall take precedence over the policy established in this instruction, except where a security requirement is more restrictive in this instruction.

7. Roles and Responsibilities

a. Designated Approving Authority (DAA). The Secretary of the Navy is the Departmental DAA per reference (b) and therefore possesses authority to formally assume responsibility for operating systems at an acceptable level of risk. This term is synonymous with "designated approval authority" and "delegated accrediting authority." The DAA formally grants authority to operate information technology resources/systems based upon an acceptable level of risk. The DAA reviews and approves security safeguards and countermeasures for information technology and issue accreditation statements, to include all information technology resources under the DAA's jurisdiction.

b. Senior Information Assurance Officer (SIAO). The DON Chief Information Officer (DON-CIO) is the designated DON SIAO, and has been delegated DAA authority for the DON.

c. Local IA Authorities. OJAG and CNLSC are local IA authorities and required to implement IA policy within their organizations pursuant to reference (c), which includes responsibility for:

(1) Designating in writing a Command Information Officer (CIO), IA Manager (IAM), and IA Officers (IAO) responsible for compliance with all IA directives and policies;

(2) Ensuring systems development life-cycle incorporates IA and interoperability to maximize security and interoperability returns on the investment;

(3) Developing IT security POA&Ms in accordance with reference (b) to delineate and schedule tasks necessary to resolve identified IA security and program weaknesses, as well as to assess, prioritize, and monitor the progress of resolving identified weaknesses.

(4) Oversight and management of organization IA training programs;

(5) Requesting vulnerability assessment assistance;

(6) Validating IA policy implementation through formalized IA checklists, assessments and inspections.

d. Command Information Officer (CIO)

(1) Code 65 is designated the OJAG/NLSC CIO and delegated responsibility for implementing the OJAG/CNLSC IA Program consistent with Local IA Authority duties identified above, and in accordance with DOD and DON IA policy.

(2) The OJAG/NLSC CIO shall:

(a) Ensure compliance with DOD and DON IA policy to ensure complete IA Readiness within the OJAG/CNLSC organizations;

(b) Perform routine risk assessments of OJAG/NLSC information systems and IA programs;

(c) Ensure compliance with Accreditation and Certification standards, as well as timely and successful approval of requests to DON DAA for Authority to Operate (ATO) and Interim ATO (IATO) OJAG/NLSC IA systems or programs;

(d) Oversee the IA Workforce and qualifications;

(e) Oversee IAM functions and management of the IA Program; and,

(f) Recommend candidates for designation as the OJAG/NLSC IAM for approval by the Judge Advocate General and/or Commander, Naval Legal Service Command, or their designee.

e. <u>Information Assurance Manager (IAM)</u>. The IAM shall:

(1) Identify security deficiencies and, if serious enough to preclude accreditation, take appropriate corrective action to eliminate the deficiencies to achieve an acceptable level of security;

(2) Ensure all safeguards and countermeasures (e.g., Port security and host-based network scanning) required to maintain an acceptable level of risk are implemented and maintained;

(3) Ensure accompanying security staff (i.e., OJAG/NLSC Network Security Officer (NSO), Systems Administrator, IA Officers) are formally appointed and receive formal IA training to carry out the duties and assigned functions;

(4) 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;

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

(6) Ensure IT, information and network security protocols meet current DoD and DON standards while also enabling the most efficient performance of authorized tasks;

(7) Ensure users receive access only to the information, resources and systems necessary for the performance of assigned functions to which they are authorized by virtue of their billet, position and security clearance;

(8) 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;

(9) Draft for CIO approval and execute Contingency Plans for all acquired information technology regarding events such replacement of systems or components, systems configuration, disaster recovery, and IT personnel manning, etc.;

(10) Ensure that IA awareness, training, education, and IA certification are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities;

(11) Assist Physical Security Officers in the implementation of Public Key Infrastructure (PKI) requirements and policy.

(12) Implement IA policy in accordance with references (a) through (c), including the promulgation of formal checklists for compliance, assessment, and inspection.

f. Information Assurance Officers (IAO)

(1) NLSC Commanding Officers will designate in writing Information Assurance Officers (IAOs) to serve as local representatives to coordinate with the IAM in the execution of the IA Program. They will forward such designations to the OJAG/NLSC CIO who will validate in writing that IAOs have completed requisite training and certification to perform IAO responsibilities and duties.

(2) The Assistant Judge Advocate General, Operations and Management (Code 06) will designate an IAO for OJAG/NLSC Headquarters.

(3) IAO responsibilities and duties will be specified in designation letters tailored to each command's size and capabilities and may include:

(a) Complete IAO training to increase knowledge of IA and to understand the possible risks and vulnerabilities, and provide course completion certificates to the OJAG/NLSC IAM.

(b) Ensure all covered personnel with access to information technology actively both participate in IT and information system security education and user awareness training programs in accordance with Public Law 100-235 (Computer Security Act of 1987), and have signed user agreements.

(c) Ensure that all software updates and security patches have been implemented on all non-networked computers on a monthly basis or more often, if needed, based on information provided by the OJAG/NLSC IAM.

(d) Maintain a local inventory of all IT assets to include desktops, laptops, printers, scanners, external hard drives and other external storage devices.

(e) Ensure compliance with all DoN CIO, NAVCYBFORCOM and other DON IA guidance with direction from OJAG Code 65.

(f) Ensure that all IT assets are disposed of properly in coordination with OJAG Code 65.

g. Information Technology/System User(s). All personnel authorized to use OJAG/NLSC IT and information systems shall:

(1) Comply with the conditions and requirements of DoN User Agreements regarding IT and information systems, and comply with DoD, DON and command information system and IT policies.

(2) Complete IT and information security user awareness training and Certification programs, as required.

(3) Report any IA concerns or policy violations to the cognizant IAO, or to the OJAG/NLSC IAM or CIO if the local IAO is unavailable.

8. Action.

a. All OJAG/NLSC commands, activities and personnel shall comply with the OJAG/NLSC IA Program, and with DoD and DON IA programs and policies.

b. The OJAG/NLSC CIO) shall exercise oversight of the IA Program through the OJAG Inspector General Article 6 Inspection process.

9. Reporting. The OJAG/NLSC CIO shall develop, maintain, and collect data repositories to support the IA Program, and to provide summaries of IA program compliance, training and certification and the overall security posture of OJAG/NLSC commands and staff activities.

NANETTE DERENZI
Rear Admiral, JAGC, U. S. Navy

JAMES W. HOUCK
Vice Admiral, JAGC, U. S. Navy

Distribution:
Electronic only, via Navy Directive website
http://doni.daps.dla.mil; and the OJAG website,
http://www.jag.navy.mil

Information Assurance Program Policy

1. IA Program compliance and reporting

a. The OJAG/NLSC IAM is responsible for executing and monitoring the IA Program throughout the OJAG/NLSC enterprise and subordinate command and staff activities.

b. Designated IAOs are responsible for reporting IA and security status and/or compliance via approved incident reporting and inspection systems, and via the reporting chain of command.

c. Reportable IA program information includes, but is not limited to:

- IA Training
- Information Systems Security (ISS) Accreditation
- IA Vulnerability Alerts
- Information Security Operations Conditions
- IA Incident Reporting
- Excessing Information Technology Resources
- Copyright violations
- Information Security violations
- Operations Security violations
- Communications Security violations

2. Information Technology (IT) system development

a. The OJAG/NLSC CIO, IAM, and IAO will implement and maintain an adequate level of defense-in-depth and defense-in-breadth security for all information technology resources (i.e., Information Systems (IS), applications, networks) under their cognizance.

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

c. Acquisition and procurement specifications must identify security requirements as part of the Information System Security (ISS) process planning, approval and execution requirements for acquisitions and procurements, in accord with Information Assurance Certification And Accreditation (C&A)

guidance under the DON Information Assurance Publication Module 5239-13 Vol. II (rev 01) (www.inforsec.navy.mil).

d. Computer security will be built into systems so that user responsibility to develop security procedures and controls for their system is minimized.

e. The OJAG/NLSC CIO shall establish policy for the procurement and management of IT assets, to include hardware and software. All purchases shall be pre-approved by the OJAG/NLSC CIO 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;

(a) CD-ROM disks and floppy disks may be procured without OJAG/NLSC CIO pre-approval.

(b) Removable storage media such as thumb drives, flash drives, external hard drives must be approved for purchase by the OJAG/NLSC CIO.

(2) Computers and IT devices. All computer purchases must come through OJAG Code 65 for initial load of IA software such as antivirus software, excepting computers and computer assets supplied through NMCI. 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 65. Further updates and security patches will be performed by Command IAOs. OJAG Code 65 will maintain an inventory of all computers, laptop and desktops throughout OJAG/NLS;

(3) Software

(a) Code 65 will approve all software purchases.

(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 whom violate OJAG/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 OJAG/NLSC Configuration Manager (CM).

3. Information Security.

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

b. All computer resources that process or handle classified information, information critical for the command's mission, or sensitive unclassified information shall contain the appropriate mission assurance category (MAC), and confidentiality levels as established within the nine baseline IA levels that may coexist within the Global Information Grid (GIG). Baseline IA levels are achieved by applying the specified set of IA Controls in a comprehensive IA program that includes acquisition, proper security engineering, connection management, and IA administration.

c. Additional guidance for NLSC Information Security programs and procedures is contained in the Naval Legal Service Command Manual at COMNAVLEGSVCCOMINST 5800.1F of 6 Oct 2010.

d. A complete listing of DoD and DON Information Security policies and instructions is available at: https://infosec.navy.mil/.

e. 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

f. 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. Printed reports shall be labeled in accordance with SECNAVINST 5510.3B.

4. Operations and Communications Security. In all electronic and other communications, all personnel must comply with DoD, DON and OJAG/NLSC programs regarding Operations Security (OPSEC) and Communications 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.

5. Computer Network Defense (CND) and Countermeasures. Information Assurance and CND are linked together as operational concepts for all echelons of the chain of command to ensure the security of information, data and computer networks that are vital to DoD/DON Homeland Defense missions and national security. NLSC Commanding Officers shall coordinate with the OJAG/NLSC CIO and with Regional Network Security activities for approval before implementing IA countermeasures to protect local IT assets or networks.

DEFINITIONS

Accreditation. The formal management authorization for operating of a specific business system application, network or computer resource, based on the results of a security certification and risk assessment. It is a formal declaration by the Designated Approving Authority (DAA) that the information technology/system is approved to operate in a particular security environment meeting a prescribed set of security requirements.

Audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operations procedures, and to recommend changes in controls, policies, or procedures.

Certification. This is the formal technical evaluation of security features and other safeguards, made in support of the accreditation process, which establishes the extent to which a specific application of an information system, network or computer resource meets a set of specified technical security requirements.

Certification Authority. Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation package.

Communication Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation or access to computer networks, information systems or their contents or theft of information. CND protection activity employs LA protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND services, intelligence, counterintelligence and law enforcement. CND response can include recommendations or actions by network operations (including LA), restoration priorities, law enforcement, military forces and other US Government agencies. (Ref (b))

Configuration Management. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

Data Integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Designated Approving Authority (DAA). The authority who decides that an information technology, network and/or computer resource may operate based on an acceptable level of risk considering the operational need for, and threats to, the system. The DAA is also responsible for issuing an accreditation statement that records the decision.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities.

Information Assurance (IA). The technical and managerial measures of protecting information and information systems by ensuring confidentiality, integrity, availability, authentication, and non-repudiation. This also includes disaster recovery, and continuity of operations. See reference (c), paragraph 4.b.

Information Security (INFOSEC). The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.

Information System (IS). An assembly of computer hardware, software, and/or firmware configured to collect, create, disseminate, process, store and/or control data or information.

Information System Security. Protection of information systems against unauthorized access to information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Information System Security Incident. Information system security incidents are events that have actual or potential adverse effects on information systems. Some examples of adverse effects are:

- Unauthorized Access
- Denial of services
- Loss of data

Information System Security Officer (ISSO). The person responsible to the DAA for ensuring the security of an information system throughout its life cycle, from design through disposal.

Information System Security Plan (ISSP). A required document used to establish and/or update the activity information system security plan. It should promulgate information system security policy and provide guidelines to be used by the activity (i.e. document the current information system security environment, establish program objectives, and outline a plan of action and milestones to achieve full accreditation).

Information Technology (IT). The hardware, firmware, and software used as part of the information system to perform DoD information functions. This includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

Interim Approval To Operate (IATO). Temporary approval granted by a DAA for an information system to process information based on preliminary results of a security evaluation of the system.

Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

Public Key Infrastructure (PKI). PKI is a framework of laws, policy, procedures and technology for the use of digital credentials, which provide: confidentiality, integrity, authentication, non-repudiation in electronic communications and transactions.

Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

Risk Assessment. Process of analyzing threats to and vulnerabilities of an information system and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and cost-effective measures.

Risk Management. Process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.

Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

Security Inspection. Examination of an information system to determine compliance with security policy, procedures, and practices.

Security Process. The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life cycle.

Security Requirements. Types of levels of protection necessary for equipment, data, information, applications, and facilities to meet the security policy.

Security Requirements Baseline. Description of the minimum requirements necessary for an information system to maintain an acceptable level of security.

Security Specification. Detailed description of the safeguards required to protect an information system.

Security Test and Evaluation (ST&E). Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.

Sensitive Information. Data which the loss, misuse, or unauthorized access to or modification of, could adversely affect national interests, the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (Privacy Act). Sensitive information is data which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

System. The set of interrelated components consisting of mission, environment, and architecture as a whole.

System Integrity. The attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Authorization Agreement (SSAA). The SSAA is a formal agreement between the DAA(s), the Certifier, user representative, and program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operation systems security.

User (or Information System User). Person or process authorized to access and utilize information system.

User Representative. The individual or organization that represents the user or user community in the definition of information system requirements.

Validation Phase. The process by which users, acquisition authority, and DAA agree on the correct implementation of the security requirements and approach for the completed information system.

Verification Phase. The process of determining compliance of the evolving information system specification, design, or code with the security requirements and approach agreed upon by the users, acquisition authority, and DAA.

Vulnerability. Weakness in an information system, system security procedures, internal controls, and/or implementation that could be exploited.

Vulnerability Assessment. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.