DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

IN REPLY REFER T
OPNAVINST 5239.1C
N6
20 Aug 08

OPNAV INSTRUCTION 5239.1C

From: Chief of Naval Operations

Subj: NAVY INFORMATION ASSURANCE (IA) PROGRAM

Ref: (a) Federal Information Security Management Act (FISMA), Title III, E-Government Act (Public Law 107-347)
(b) DoD 5220.22-M, 28 Feb 06
(c) DoD Directive 8500.01E, 24 Oct 02
(d) SECNAVINST 5239.3A
(e) DoD Instruction 8500.2, 6 Feb 03
(f) OPNAVINST C5510.93F/MCO 5510.19 (NOTAL)
(g) DoD Instruction 8520.2, 1 Apr 04
(h) SECNAVINST M-5239.1
(i) Committee for National Security Systems (CNSS) Instruction 4009
(j) DoD Instruction (DoDI) 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), 28 Nov 2007
(k) DoD Instruction O-8530.2, 9 Mar 01
(l) DoD Directive O-8530.1, 8 Jan 01
(m) CJCSM 6510.01
(n) OPNAVINST 3100.6H (NOTAL)
(o) DoD Directive 5000.01, 12 May 2003
(p) DoD Instruction 5000.2, 12 May 2003
(q) DoD 8570.01-M, 19 Dec 05
(r) DoD Directive 3020.40, 19 Aug 2005
(s) Strategic Command Directive (SD) 527-1

Encl: (1) Acronyms

1. Purpose. This instruction establishes policies and procedures for the Navy's Information Assurance (IA) program. It implements the provisions of references (a) through (g). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. Office of the Chief of Naval Operations Instruction (OPNAVINST) 5239.1B.

3. Applicability

a. This instruction applies to all Navy activities, organizations, and contractors that:

(1) Use Navy information systems which receive, process, store, display or transmit Department of Defense (DoD) information, or;

(2) Process data or information described in paragraph 3a, including classified and unclassified and not limited to National Security Information as defined in reference (a), or;

(3) Operate systems on behalf of DoD or own facilities or systems that process classified and unclassified information associated with Navy contracts. Contractors processing classified information shall also comply with reference (b).

b. Nothing in this policy shall alter or supersede the existing authorities and policies of the Director of National Intelligence and Deputy Chief of Naval Operations, Intelligence (CNO (N2)), as the Navy Senior Official of the Intelligence Community (SOIC), regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 and other laws and regulations in accordance with references (c), (d) and (h).

4. Background

a. Reference (h) states that IA shall be achieved through the cost-effective, risk-balanced application of controls in a manner that promotes confidentiality, integrity, availability, non-repudiation, and authentication of information.

b. To help further delineate the distinction between IA and Computer Network Defense (CND), the following definition of IA will be adopted Navy-wide. IA is 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.

c. The five attributes of IA, defined in references (h) and (i), are:

(1) Confidentiality. Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

(2) Integrity. Quality of an information system is 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. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

(3) Availability. Timely, reliable access to data and information services for authorized users.

(4) Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

(5) Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

d. The security challenges confronting Navy information and information systems are multiplying rapidly with the growth of interconnected systems forming the Global Information Grid (GIG). The threats are becoming more sophisticated and diverse, and Navy systems become inherently more vulnerable to surreptitious access, user misuse, abuse, and malicious attacks.

e. Reference (j) superseded DoD Instruction 5200.40, 30 December 1997, Department of Defense Information Technology Certification Security Certification and Accreditation Process (DITSCAP), and DoD 8510.01-M, July 2000, Department of Defense Information Technology Certification Security Certification and Accreditation Process (DITSCAP) Application Manual.

5. Objectives. Deputy Chief of Naval Operations, Communication Networks (CNO (N6)) directs the implementation of the Navy's IA program, through the policy set forth in this instruction, to:

a. Protect information and information systems to the degree commensurate with their Mission Assurance Category (MAC) and Confidentiality Level (CL).

b. Adopt an Information Technology (IT) life-cycle risk management program, including a realistic assessment of the remaining useful life of legacy systems compared with the cost of adopting current technologies.

c. Achieve and maintain C&A, or platform IT designation for Navy information systems per Navy C&A and IA policy.

6. Policy

a. The Navy IA program will meet the requirements of references (a) through (p). To accomplish this requires a continuous effort in both the operational community and in defining acquisition requirements. In accordance with references (d) and (h), the primary Navy parties responsible for implementing IA requirements are the Designated Approval Authorities (DAA) and acquisition program managers. All Navy information, telecommunication, and network systems shall be safeguarded at all times to support defense-in-depth across the GIG.

b. All Genser information system owners shall identify the MAC and CL for their systems and information per reference (c).

c. C&A policy requires all Navy information systems not designated platform IT systems to be certified and accredited as part of the acquisition process and during the system's operational life.

7. Information Assurance Publications. Navy IA publications detail roles and responsibilities for IA and IA-related matters. Navy IA publications will reflect the latest affordable, acceptable, and supportable IA and IA-related procedures and techniques. Navy IA publications provide guidance when Department of the Navy (DON), Joint, and DoD directives, manuals, and guides require additional detail or clarification for Navy-unique systems or usage.

8. Organizational Responsibilities

a. CNO (N6) ensures full implementation and coordination of Navy IA program execution with the Assistant Secretary of the Navy (Research, Development and Acquisition) and Deputy Assistant Secretary of the Navy (Command, Control, Communications, Computers and Intelligence (C4I))/Electronic Warfare/Space. To execute this responsibility, CNO (N6) will:

(1) Represent Navy as the governing individual for all Navy IA programs.

(2) Appoint the Commander, Naval Network Warfare Command (NNWC) as the Navy Operational DAA (ODAA) for collateral/General Services (GENSER) classified and unclassified, operational information systems, networks, and telecommunications systems.

(3) Appoint Special Program Division (OPNAV (N89)) as the DAA and Computer Network Defense Service Provider (CNDSP) for all special access program systems.

(4) Appoint Director, Office of Naval Intelligence (ONI) as the Navy liaison to the National Security Agency (NSA) DAA for all SCI program systems.

(5) Appoint Navy second echelon commanders as Developmental DAAs (DDAAs) during the information, telecommunications, or network system's acquisition and development phase, prior to any operational deployment or connection to operational networks. Further delegation of this DAA authority to specific acquisition program managers is limited to officers of the grade of O-6 or above and U.S. government personnel grade GS-15 or above or equivalent, unless coordinated with and authorized by CNO (N6) in advance.

(6) Appoint Commander, Space and Naval Warfare Systems Command (SPAWAR), as the Navy's Certification Authority (CA) for collateral/GENSER classified and unclassified, information, telecommunications, and network systems.

(7) Sponsor, authorize, and budget for IA requirements.

(8) Approve and issue the Navy's IA policy, systems management, and metrics documents, to include policy for the CA, ODAA, and DDAA.

(9) Represent Navy interests on various international, national, DoD, and Navy groups that develop IA policy. CNO (N6) shall periodically review its priorities and then ensure that Navy IA is represented at key groups.

(10) Coordinate with CNO (N2), as the Navy SOIC, and his cognizant security authority on issues of common concern regarding implementation of IA policies (Director of Central Intelligence Directive (DCID) 6/1, Security Policy for Sensitive Compartmented Information and Security Policy Manual, 1 March 1995; DOD 5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual, August 1998; and Secretary of the Navy Instruction (SECNAVINST) 5510.36A, DON Information Security Program (ISP) Instruction, 6 October 2006, are germane).

(11) Oversee Navy IA training requirements and provide requirements to the Personnel and Training Standing Team (PTST) Working Group.

(12) Plan, resource, and provide oversight on IA capabilities well in advance of their projected deployment. This anticipatory planning recognizes that IA capabilities require threat anticipation, specialized development, unique acquisition skills, and additional time for C&A. Most often, centralized IA acquisition processes provide the most economical and secure implementation, especially for high assurance products. CNO (N6) will review and support business cases when independent procurement may provide a more economical solution while maintaining the same product IA robustness.

(13) Identify Navy IT and telecommunication critical assets and infrastructures in accordance with reference (j).

(14) Coordinate fleet requirements for the acquisition of Communications Security (COMSEC) material for DON.

(15) Draft and maintain the Navy's IA master plan document in accordance with references (c) and (h). This document shall be jointly authored by the Navy's acquisition

program manager, the Navy's CA, NNWC, and CNO (N6), as part of the IA requirements process. It serves as the means to consolidate and prioritize IA requirements, update Navy-wide IA and IA-related policies, and delineate IA and IA-related acquisition responsibilities and programs.

(16) Draft and maintain the Navy's IA documents in accordance with reference (e). This standards section shall serve as a mandated IA standards reference for all other program architectural Technical Views (TV-1 and TV-2) and Navy IA standards input to the Defense Information Standards Registry.

(17) Submit program objectives memorandum requirements to support IA programs as delineated in the Navy IA documents cited in paragraph 8a(16).

(18) Appoint a classification authority to ensure DoD data is protected in accordance with appropriate MAC/CL.

b. Commander, NNWC, in conjunction with its subordinate commands: Navy Information Operations Center (NIOC) Norfolk, Naval COMSEC Material System (NCMS), and Navy Cyber Defense Operations Command (NCDOC) shall:

(1) Annually gather Navy IA operational requirements from all echelon II commands. Prioritize the requirements and submit a consolidated listing to CNO (N6).

(2) Serve as the ODAA for all operational Navy GENSER IT systems, networks, and telecommunication systems.

(a) Provide guidance to DDAAs for implementation of Navy C&A policy and for implementation of IA controls on systems exempt from the C&A process.

(b) Coordinate Defense Information Infrastructure (DII) connection approval with the Defense Information Systems Agency (DISA) for Navy information systems and sites. Ensure sites with DII connections meet DISA accreditation requirements. Utilize NIOC and Commander, Operational Test and Evaluation Force (COMOPTEVFOR) as the operational test agents as applicable and necessary.

(3) Oversee operation of Navy networks including monitoring and restoration functions.

(4) Coordinate with NSA and Defense Intelligence Agency (DIA) for C&A of information operations/signals intelligence systems and networks.

(5) Coordinate the Navy Service Cryptologic Element IA and IA-related program activities with the NSA.

(6) Provide CND training to fleet units as requested by fleet commanders on an annual basis.

(7) Conduct Carrier Strike Group and Expeditionary Strike Group Computer Network Vulnerability Analysis (CNVA) training and testing. Establish memorandums of agreement with fleet commanders for this training. Provide metrics data to CNO (N6) that measures the IA readiness (lower risk) for platforms both before and after receiving CNVA support.

(8) Serve as Navy lead for ports, protocols, and services management.

(9) Serve as the computer network vulnerability testing agent for the Navy enterprise and legacy networks. This includes technical evaluations, operational evaluations, verification of correction of deficiencies, and service level agreement testing.

(10) Serve as testing agent for COMOPTEVFOR as part of the vulnerability analysis for new equipment and networks prior to fleet deployment and DAA accreditation.

(11) Conduct penetration testing and vulnerability analysis during military exercises, as required. This activity includes validating security compliance, DISA standards implementation, IA Vulnerability Management (IAVM) compliance, and the overall system IA posture.

(12) Perform Web risk assessment and analysis on all Navy networks. Coordinate and direct appropriate actions to ensure that Navy web pages resident on the World Wide Web comply with prescribed DoD and Navy guidance.

(13) In accordance with references (k), (l), and (m), serve as the Navy's Tier 2 CNDSP.

(a) Coordinate the defense of Navy computer networks and information systems as directed by the Commander, Joint Task Force for Global Network Operations (JTF-GNO) and CNO (N6), and Intelligence Community - Incident Response Center (IC IRC) for SCI computer networks and information systems. For SCI computer networks and information systems on NSAnet, additional coordination is required with NSA's Central Security Service Information Systems Incident Response Team, and on Joint Worldwide Intelligence Communication System, additional coordination is required with DIA Department of Defense Intelligence Information Systems Information Assurance Protection Center. Reporting of all incidents affecting Navy SCI computer networks and systems to (CNO (N2)) and Special Security Office Navy is required in addition to JTF-GNO and IC-IRC reporting requirements.

(b) Determine when system(s) are under strategic computer network attack, contain damage, restore functionality, and provide feedback from forensic studies to the user community.

(c) Execute all actions required to protect, monitor, analyze, detect and respond to unauthorized activity within Navy information systems and computer networks.

(d) Coordinate Navy efforts with other government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and information systems, and to minimize or eliminate identified vulnerabilities.

(e) Develop and maintain an infrastructure that has the capacity and capability to maintain raw data required for forensics and trend analysis.

(f) Make Information Operations Condition (INFOCON) recommendations and report the Navy INFOCON status per reference (n).

(g) Coordinate Red Team exercises to de-conflict exercise and real world activity as necessary; analyze Red Team

exercise results and incorporate lessons learned into NCDOC directives and guidance to subscribers for vulnerability mitigation; and receive Red Team exercise After Action Reports and confirmation of command implementation of required actions.

(14) Coordinate with other service and national level organizations and agencies to share information concerning vulnerabilities, threats, countermeasures and Navy computer network security incidents.

(15) Develop contingency plans, tactics, techniques, and procedures to defend Navy computer networks; support deliberate planning efforts as directed by JTF-GNO. Operate a 24/7 computer incident response team to centrally coordinate actions involving computer network security incidents and vulnerabilities, which threaten Navy computer networks worldwide.

(16) Monitor the IA readiness of Navy computer networks and maintain a global CND user defined operational picture for situational awareness.

(17) Provide the intelligence community with priority intelligence requirements for collection and Indications and Warning (I&W) requirements for potential attacks against Navy computers and networks.

(18) Oversee and conduct the vulnerability analysis and assessment program for the Navy.

(19) Resource, train, and coordinate flyaway support as required in response to Navy network security incidents.

(20) Report all computer network incidents evaluated as being of interest to Navy officials to higher authorities via priority message. Report any event or incident evaluated as a computer network attack with significant or severe operational impact to the CNO (N6) via Operational Report-3.

(21) Participate in Joint and Navy training exercises and refine CND tactics, techniques, and procedures.

(22) Publish monthly, quarterly, and annual summaries of reported Navy computer incidents.

(23) Provide timely advisories for newly identified vulnerabilities.

(24) Manage the Navy's IAVM program per reference (m) and act as the Navy's reporting agent for IAVM and computer tasking orders.

(25) Maintain the central office of record, ensuring the proper storage, distribution, inventory, accounting, and overall safeguarding of COMSEC materials for the Navy, Marine Corps, Coast Guard, Military Sealift Command, and joint and allied commands, as required.

(26) Control, warehouse, and distribute cryptographic equipment, ancillaries, and associated keying material for all Navy.

(27) As DON COMSEC policy author, write safeguarding and accounting policies for DON COMSEC material. Review, issue, publish, and distribute guidance necessary to ensure National level (e.g., NSA) policies are followed and enforced.

(28) Serve as the Navy's High Assurance (Class 4) Public Key Infrastructure (PKI) certificate approving authority.

(29) Serve as a Navy registration authority for Medium Assurance (Class 3) PKI.

(30) Serve as the DON COMSEC incident monitoring activity.

(31) Manage the DON COMSEC Inspection Program. Establish standards for COMSEC inspectors and inspections.

(32) Manage the DON COMSEC Training Program. Provide worldwide COMSEC advice and assistance to customers.

(33) Resolve COMSEC related technical queries and conflicts with members of DON and national COMSEC community.

c. Program Executive Office (PEO) C4I, will serve as the Navy's IA acquisition program manager and overall systems

security engineering lead and the Navy's lead on joint and coalition interoperability of IA capabilities shall:

(1) Manage the Navy's IA acquisition programs and projects, including associated research and development and full life-cycle systems support in accordance with references (d), (o), and (p). Ensure coordination with DISA and other services on the procurement of DoD-wide IA and IA-related products and licenses that may be deployed on Navy networks.

(2) Serve as the Navy's CND technical manager and CND systems integrator in accordance with references (k) and (l) and provide technical support to the Navy's CND architect.

(3) Provide systems and security engineering, integration testing, and support for all Navy information telecommunication, and network systems. Serve as the Navy's technical lead for IA and IA-related products and services used within ship, aircraft, and shore IT systems, including Navy-Marine Corps Intranet and ONE-net. Provide security engineering services for protection of critical IT assets and telecommunications infrastructures.

(4) Provide input, review, and recommended updates to IA publications.

(5) Support NNWC in all efforts to protect information, telecommunication, and network systems.

(6) Serve as the focal point and technical lead for Navy IA research and development. Work closely with the Office of Naval Research and the Naval Research Laboratory to identify basic research programs that can be transitioned to operational use to satisfy documented IA requirements.

(7) Provide IT system security engineering and other technical support to the Navy's CA for all service, joint, and coalition programs.

(8) Serve as the Navy's technical lead for the development and maintenance of IT risk management programs.

(9) Provide security system engineering services to other PEO's and program managers for system C&A.

(10) Maintain the Navy Information Security (INFOSEC) Web site and IA help desk.

(11) Provide technical assistance to NNWC on standards and content associated with training requirements for the Navy IA workforce.

(12) Work with the Navy's spectrum office on spectrum and electromagnetic environmental effects related matters that may impact transmission security and emission security.

(13) Serve as the Navy's technical lead on the implementation of International Organization for Standardization 15408, Common Criteria program.

(14) Serve as technical support to the Navy's representative on the United States Strategic Command Enterprise-wide Solutions Steering Group.

(15) Serve as the Navy COMSEC systems technical lead and acquisition authority. This includes:

(a) Centralized specification and technical approval of all Navy high and medium robustness COMSEC devices and systems, such as those implementing Federal Information Processing Standard 140 and NSA Suites A and B algorithms. This includes central procurement of all high robustness cryptographic equipment that receives CNO (N6) requirement validation. The central acquisition authority role includes U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, and the Military Sealift Command.

(b) Serve as the Navy's cryptographic modernization program office.

(c) Execute acquisition programs to ensure an effective key management infrastructure for the above systems.

(d) Provide technical support to NCMS.

(16) Execute acquisition and implementation programs to ensure that the Navy has effective PKI and Public Key (PK) enabling efforts.

(17) Act as the lead office for implementing and executing the DON Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) Program.

(18) Support CNO (N6), NNWC, and SPAWAR on all IA technical issues.

d. Commander, SPAWAR, as the Navy's GENSER CA, shall:

(1) Provide high-level oversight and standardization for information system C&A processes for all IT systems, sites, and networks requiring C&A under the DON IA policy.

(2) Provide technical and non-technical system security evaluations to determine operational risk to Navy networks.

(3) Recommend C&A approvals or denials to the appropriate DAA.

(4) Provide procedural guidance on the C&A process.

(5) Support CNO (N6) policy development on C&A process and related issues by document reviews and draft inputs.

(6) Maintain metrics and provide feedback on cyclical process improvement to C&A communities of interest.

(7) Provide training requirements input to appropriate training authorities for enhancement of C&A community members.

(8) Serve as the Navy's IA Technical Authority (TA) following SECNAVINST 5400.15C of 13 September 2007.

(a) Execute TA, which is the authority, responsibility and accountability to establish, monitor and approve technical standards, tools and processes in conformance to higher authority policy, requirements, architectures and standards, in accordance with Virtual Systems Command (SYSCOM) Joint Instruction - VS-JI-22A of 31 January 2007.

e. Commanders of SYSCOMs, PEOs, and other Navy development and acquisition activities shall ensure program managers

integrate IA requirements in the design of information systems that meet C&A responsibilities.

f. The PTST Working Group, established, shall:

(1) Identify Navy IA billet and training requirements.

(2) Ensure development of Navy training plans for information systems.

(3) Establish IA training requirements for military and civilian personnel.

g. Commander, Naval Education and Training Command, shall:

(1) Develop Navy schoolhouse IA training and education.

(2) Ensure IA training is incorporated into all pertinent Navy training and appropriate formal schools.

h. Director, ONI, shall:

(1) Assist CNO (N6) and PEO C4I in the risk management process by gathering relevant threat information to assist in defining system security requirements.

(2) Provide all-source cyber collection and analysis, fused intelligence support to NNWC.

(a) Deliver in-depth trend analysis for I&W of computer attacks/exploitation of National/Navy networks.

(b) Provide all sources targeting to more effectively leverage full spectrum of collection means. (References OPNAVINST 3811.1D and OPNAVINST 5450.334 germane.)

(3) Assist CNO (N6) and PEO C4I in the risk management process by gathering relevant threat information to assist in defining system security requirements.

(4) Provide all-source, fused intelligence support to NNWC.

i. Naval Criminal Investigative Service shall provide law enforcement and counter-intelligence support for computer crimes and compromises of classified information to any command through the following processes: conducting investigations, operations, proactive programs, and related analyses of cyber incidents and targeting involving DON IT assets; collecting, tracking, and reporting on threats to DON IT assets; and by supporting and conducting cyber-related criminal investigations.

j. Second echelon commanders shall implement the Navy's IA program within their respective commands and areas of responsibility. This includes:

(1) Appoint in writing a Command Information Officer (CIO). CIOs are responsible for compliance with all IA directives and policies, and shall ensure the systems development life cycle incorporates IA and interoperability to maximize security and interoperability returns on the investment.

(2) Appoint in writing Information Assurance Managers (IAMs) and other appropriate IA positions.

(3) Appoint in writing Information Assurance Officers (IAO) to assist the IAM, to oversee systems or to oversee networks and other IT and telecommunications systems.

(4) Provide oversight and management of the activity IA training program in accordance with all policies stated and referred to by this instruction, to include the Navy IA manuals.

(5) Request vulnerability assessment assistance from NCDOC and Red and Blue Team operations from NIOC Norfolk to validate IA controls and practices.

(6) May serve as DDAA for command area of responsibility. DDAAs must meet the requirements of reference (c) for DAA. ODAA must be notified in writing of the designation for each DDAA.

(7) Validate implementation of IA policy through formalized IA checklists (assessments and inspections).

(8) Ensure all sites within their echelon are fully accredited by the Navy's ODAA.

k. Commanding officers, commanders, officers-in-charge, and directors, in their role as local IA authorities, are responsible for the overall implementation of IA at the command level per references (c) through (e), (g) through (j), (n), and (q) through (s), the Navy's IA publications, and this instruction and shall:

(1) Ensure that all operational IT, networks, and telecommunications systems are fully accredited by the Navy's ODAA prior to use.

(2) Ensure all personnel performing IA functions (IA workforce) receive initial basic and system specific training, obtain required certification, and complete annual recurring, refresher, or follow-on training per reference (q).

(3) Appoint, in writing, all IA workforce personnel to include:

(a) Command IAM that reports directly to the command on all matters involving IA. Where management and administrative functions have been consolidated within a Navy organization, only the higher-level organization may designate or consolidate IAM functions as approved by Navy ODAA.

(b) IAO for each information system and network in the organization, who is responsible for implementing and maintaining the site's information system and network security requirements. For smaller commands, the same individual may perform IAM and IAO duties.

(c) System administrators as appropriate based on the number of systems the command manages.

(4) Ensure IA awareness indoctrination and annual IA refresher training are tailored to specific site requirements, completed by all users, and retain documentation. Each user shall complete the Navy's User Acknowledgement form posted on the INFOSEC Web site and record completion of training.

(5) Ensure any computer intrusion incident, or suspicion of one, is reported per reference (m) and Navy policy including reference (n). Reports include the operational chain of command for situational awareness as required by reference (m).

(6) In coordination with the ODAA, when the unit is deployed, serve as deployed DAA.

(7) Ensure C&A team members are assigned in accordance with reference (j).

9. Action. All action addressees shall implement the guidance contained herein and all associated references to include the Navy's IA publication series. All developing and operating activities shall budget for, fund, and execute the actions necessary to comply with this instruction and the publications that support it.

10. Records Management. All records created by this instruction, regardless of media, shall be managed in accordance with SECNAV Manual 5210.1.

11. Reports. The requirements contained in paragraph 8 are exempt from information collection control by SECNAV M-5214.1 and requires no Report Control Symbol.

David W. Weddel
Deputy Chief of Naval Operations
Communication Networks (N6B)

Distribution:
Electronic only, via Department of Navy Issuances Web site
http://doni.daps.dla.mil/

# Acronyms

| | |
|---|---|
| AOR | Area of responsibility |
| ASN | Assistant Secretary of the Navy |
| C4I | Command, Control, Communications, Computers, and Intelligence |
| CA | Certifying Authority |
| C&A | Certification and Accreditation |
| CIMA | COMSEC Incident Monitoring Activity |
| CISN | Communications, Information Systems, and Networks |
| CL | Confidentiality level |
| CMPO | Crypto Modernization Program Office |
| CND | Computer Network Defense |
| CNDSP | Computer Network Defense Service Provider |
| CNO | Chief of Naval Operations |
| CNSS | Committee on National Security Systems |
| CNVA | Computer Network Vulnerability Analysis |
| COMOPTEVFOR | Commander, Operational Test and Evaluation Force |
| COMSEC | Communications Security |
| COR | Central Office of Record |
| CSG | Carrier Strike Group |
| CTO | Computer Tasking Order |
| DAA | Designated Approving Authority |
| DASN | Deputy Assistant Secretary of the Navy |
| DDAA | Developmental Designated Approving Authority |
| DIA | Defense Intelligence Agency |
| DIACAP | Department of Defense IA Certification and Accreditation Process |
| DIAP | DoD Information Assurance Panel |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| DII | Defense Information Infrastructure |
| DISA | Defense Information Systems Agency |
| DoD | Department of Defense |
| DODIIS | DoD Intelligence Information System |
| DON | Department of the Navy |
| E3 | Electromagnetic environmental effects |

| | |
|---|---|
| EW | Electronics warfare |
| ESG | Expeditionary Strike Group |
| ESSG | Enterprise-wide Solutions Steering Group |
| EMSEC | Emission Security |
| FISMA | Federal Information Security Management Act |
| GENSER | General Services |
| GIG | Global Information Grid |
| I&W | Indications and Warning |
| IA | Information Assurance |
| IASL | Information Assurance Senior Leadership |
| INFOSEC | Information Systems Security |
| INFOCON | Information Operations Condition |
| IAM | Information Assurance Manager |
| IAO | Information Assurance Officer |
| IAP | Information Assurance Panel |
| IAVM | Information Assurance Vulnerability Management |
| IO | Information Officer |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| JTF-GNO | Joint Task Force for Global Network Operations |
| KMI | Key management infrastructure |
| MAC | Mission Assurance Category |
| MCEB | Military Communications-electronics Board |
| N6 | Naval Operations |
| NCDOC | Navy Cyber Defense Operations Command |
| NCIS | Naval Criminal Investigative Service |
| NIOC | Navy Information Operations Command |
| NISPOM | National Industrial Security Program Operating Manual |
| NCMS | Naval COMSEC Material System |
| NNWC | Naval Network Warfare Command |
| NSA | National Security Agency |
| ODAA | Operational Designated Approving Authority |
| ONE-net | OCONUS Navy Enterprise Network |
| ONI | Office of Naval Intelligence |
| OPNAV | Office of the Chief of Naval Operations |
| PEO | Program Executive Office |
| POM | Program Objectives Memorandum |

| | |
|---|---|
| PK | Public Key |
| PKI | Public Key Infrastructure |
| RD&A | Research, Development and Acquisition |
| SAP | Special Access Programs |
| SCE | Service Cryptologic Element |
| SCI | Sensitive Compartmented Information |
| SIGINT | Signals intelligence |
| SIOP | Single Integrated Operations Plan |
| SLA | Service Level Agreement |
| SPAWAR | Space and Naval Warfare Systems Command |
| TRANSEC | Transmission security |
| UDOP | User Defined Operational Picture |
| USSTRATCOM | United States Strategic Command |
| WRA | Web Risk Assessment |