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

IN REPLY REFER TO

OPNAVINST 5239.1B
N6
9 November 1999

OPNAV INSTRUCTION 5239.1B

From: Chief of Naval Operations
To: All Ships and Stations (less Marine Corps field addresses not having Navy personnel attached)

Subj: NAVY INFORMATION ASSURANCE (IA) PROGRAM

Ref: (a) SECNAVINST 5239.3 of 14 Jul 95, Department of the Navy Information Systems Security (INFOSEC) (NOTAL)
(b) DoD 5220.22-M of January 95, National Industrial Security Program Operating Manual (NISPOM)
(c) Public Key Infrastructure Roadmap for the Department of Defense, Version 2.0, Revision C, June 15, 1999
(d) CNO N64 Attack, Protect, Exploit Requirements Action Forum Charter
(e) Department of the Navy Chief Information Officer Information Technology Standards Guidance (ITSG) (NOTAL)
(f) DoD Instruction 5200.40 of 30 Dec 97, Department of Defense Information Technology Security Certification and Accreditation Process (NOTAL)
(g) CNO Memo 1500 Ser N7/8U637313 of 14 Oct 98 (Subj: Navy Communications, Information Systems, and Networks (CISN) Training Strategy to Support Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance/Information Operations (C4ISR/IO)) (NOTAL)
(h) NSTISSI No. 4012, of August 1997, National Training Standard for Designated Approving Authority (DAA) (NOTAL)
(i) OPNAVINST 2201.2 of 3 March 1998, Navy and Marine Corps Computer Network Incident Response

Encl: (1) List of Acronyms

1. Purpose. To establish policies and procedures for the U.S. Navy's Information Assurance (IA) Program, and implement the provisions of reference (a). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 5239.1A.

3. Applicability. This instruction applies to all Navy activities, organizations and contractors that enter, process, store, or transmit unclassified, sensitive but unclassified (SBU) or classified National Security information using information systems or networks at Navy activities, and to contractor operated or owned facilities under Navy authority, which shall also comply with the guidelines of reference (b). This instruction encompasses all information systems and networks that are procured, developed, modified, operated, maintained, or managed by Navy organizational elements. If information in this policy conflicts with other issued policy, the more stringent policy applies. Enclosure (1) provides a list of acronyms used throughout this instruction.

4. Background

a. Information Assurance is defined in Joint Pub 3-13 "Joint Doctrine for Information Operations" (9 October 1998) as:

"Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

b. The security challenges confronting Navy information and information systems are multiplying rapidly with the exponential growth of interconnected systems for producing and exchanging data and information. As interconnectivity increases and the threats to information and information systems become more sophisticated and diverse, Navy systems become inherently more vulnerable to surreptitious access and malicious attacks.

The fast-paced advances of technology drive Navy reliance on commercial technologies and services; however, many of these solutions may offer only minimal defense against IA threat activity and must be augmented by IA disciplines and focused management decisions to ensure protection of Navy information and information systems.

c. Information Assurance Properties and Services. Information and information systems must be properly managed and protected as required by law, regulation or treaty. Facilitating the management and protection of resources requires the appropriate implementation of security measures providing the IA properties and services of:

(1) Confidentiality, which supports the protection of both sensitive and classified information from unauthorized disclosure.

(2) Integrity, which supports protection of information against unauthorized modification or destruction.

(3) Availability, which supports timely, reliable access to data and information systems for authorized users, and precludes denial of service or access.

(4) Authentication, which supports verifying the identity of an individual or entity and the authority to access specific categories of information.

(5) Non-repudiation, which provides assurance to the sender of data with proof of delivery and to the recipient of the sender's identity, so that neither can later deny having processed the data.

d. Mission Criticality. Assessing the security requirements of any information system for the five IA properties requires a determination of the criticality of the information system to the organization’s mission, particularly the warfighter’s combat mission. Five categories of criticality are defined in reference (c), Administrative, Mission Support, and three categories classified as Mission Critical, although an information system may have components that fit in more than one category. Mission criticality is one of the key determinants of information security requirements, the level of effort appropriate to the certification and accreditation of systems, and the technologies appropriate for implementing the required safeguards.

e. Information Sensitivity. Information Assurance requirements also depend on the need to control disclosure. Disclosure may be restricted either because of national security classification levels (Confidential, Secret, Top Secret), because of Special Access (Single Integrated Operations Plan –

SIOP -- or Sensitive Compartmented Information – SCI) requirements, or for other sensitivity. Sensitive information is any information the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy of Department of Defense personnel, but that has not been specifically authorized to be kept classified. Unclassified national security information, Privacy Act data, personal information (such as medical records, fitness reports and performance evaluations), proprietary, source selection sensitive, nuclear propulsion information, operations or mission information may be considered sensitive information.

5. Objectives. The Chief of Naval Operations directs the implementation of the Navy IA program, through the policy set forth in this instruction, to:

a. Protect information and resources to the degree commensurate with their value.

b. Employ efficient procedures and cost-effective, information-based security features on all information technology resources procured, developed, operated, maintained, or managed by Navy organizational elements to protect the information on those resources. An analysis of costs and benefits should be used determine which procedures and security features are appropriate, including a realistic assessment of the remaining useful life of legacy systems compared with the cost of adding new security safeguards.

c. Adopt a risk-based life cycle management approach in applying uniform standards for the protection of Navy information technology resources that produce, process, store, or transmit information.

d. Conduct an assessment of threats, identify the appropriate combination of safeguards from the IA disciplines, and apply an appropriate level of certification and accreditation for each specific information system developed by a program office and for each site employing networks and deployed information systems.

6. Policy. All Navy information and resources shall be appropriately safeguarded at all times, to support defense-in-depth across Navy and DoD. Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, authentication, and non-repudiation based upon mission criticality, level of required information assurance and classification or sensitivity level of information entered, processed, stored, or transmitted. The safeguarding of information and information systems shall be accomplished through the employment of multi-disciplined defensive layers, as well as sound administrative and operational practices.

7. IA Requirements. IA Requirements should be validated by the Fleet Commanders-in-chief or other Echelon II Commanders and forwarded to the CNO N64 Attack/Protect/Exploit (CAPER) Action Forum, via CNO N643. The principle mission of the CAPER Action Forum is to review, clarify, define and validate certain CNO sponsored program issues and requirements for the operating forces of the United States Navy.

8. Information Assurance Publications. The IA Publication series provide specific guidance and direction on implementation of this instruction for Navy, and as such, are extensions of the policies herein. The IA publications detail specific roles and responsibilities and reflect the latest affordable, acceptable, and supportable procedures and products to ensure the security and protection of Navy information. IA Pub 01 introduces and summarizes the Department of the Navy’s approach to IA. Pub 01 is intended to foster a common understanding of IA principles, concepts, and interrelationships among system planners,

organizational managers, Information Systems Security Officers and Managers, and users. Appendix A to IA Pub 01 lists and describes the current and planned IA Pubs. The IA publications are maintained by Director, Communications Security (COMSEC) Material System (DCMS) and shall be updated routinely. The IA Pubs are available on the NIPRNET and the SIPRNET at the INFOSEC Web Site.

9. Responsibilities

a. Organizational Responsibilities.

(1) Chief Of Naval Operations (CNO). The CNO is responsible for ensuring full implementation and coordination of Navy IA Program execution with the Assistant Secretary of the Navy (ASN) Research Development & Acquisition (RD&A) and Deputy Assistant Secretary of the Navy (DASN) Command, Control, Communications, Computers and Intelligence/Electronic Warfare/Space (C4I/EW/Space). The CNO executes this responsibility by:

(a) Appointing the Navy Senior Information Systems Security Manager (SISSM) with authority as the Navy principal Designated Approving Authority (DAA) for collateral/GENSER classified and sensitive but unclassified information systems.

(b) For the Navy, the CNO has appointed the Director, Space, Information Warfare, Command and Control (N6) as the SISSM.

(c) CNO (N6) has delegated the duties of Navy SISSM to CNO (N643).

(d) Directing the SISSM to ensure execution of responsibilities outlined in reference (a) and to develop the procedures and policies necessary to implement higher directives and regulations.

(e) Appointing CNO (N89) as the DAA for all Special Access Programs.

(f) Appointing CNO (N3/N5) as the DAA for all Single Integrated Operations Plan (SIOP) programs.

(g) Appointing Director, Office of Naval Intelligence as the DAA for all Sensitive Compartmented Information (SCI) programs.

(h) Appointing Commander, Naval Security Group Command as the DAA for all cryptologic systems and SCI physical facilities under their cognizance.

(2) CNO (N643) shall:

(a) Oversee the Navy IA Program. Provide streamlined, simplified and standardized security guidance and policy.

(b) Approve and issue the Navy IA Master Plan.

(c) Represent IA Requirements submitted by Fleet Commanders-in-Chief and other Echelon II Commanders to the CNO N64 Attack, Protect, Exploit Requirements Action Forum (CAPER AF) (ref (d)).

(d) In coordination with Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) (PMW-161), develop and issue standards for critical IA components (e.g. firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs)), for use within Navy information systems and networks. Critical IA components are those which, to ensure interoperability with other Navy, joint or other DoD systems, must be standardized and managed at a service level. Standards will be documented in the DoN CIO Information Technology Standards Guidance, Chapter 3 (ref (e)).

(e) Represent CNO as the DAA for Navy-wide and joint service information systems (where Navy is the assigned lead). Assign DAAs and ensure the accreditation of all Navy information technology resources. CNO (N643) further delegates DAA authority to second echelon commanders for acquisition and development of information systems within their cognizance. Further delegation of this DAA authority is limited to officers of the grade of O-6 or above and civilians of grade GS-15 or equivalent except by prior coordination with and authorization from CNO (N643).

(f) Provide Navy representation to the DoD Information Assurance Panel, subordinate working groups and other DoD-level working groups and study groups relating to IA.

(g) Coordinate Navy submission of reports on IA postures, to include training initiatives and overall progress in meeting IA goals and objectives.

(h) Oversee Navy IA training requirements and provide requirements to the Communications, Information Systems, and Networks (CISN) Training Working Group (see item (7)).

(3) Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) (PMW-161) is the Department of the Navy’s IA Program Manager. As such COMSPAWARSYSCOM (PMW-161) shall:

(a) Ensure full coordination of Navy IA program execution with CNO (N643), COMNAVSECGRU, COMSPAWARSYSCOM (PMW-162) and Headquarters USMC.

(b) Draft and maintain the Navy IA Master Plan as requested by CNO (N643), and in coordination with CNO N64 Attack/Protect/Exploit Requirements (CAPER) Action Forum, Headquarters Marine Corps, COMNAVSECGRU, and other Naval Systems Commands. The IA Master Plan shall include identification and formal documentation of IA goals and objectives for Navy, a strategy for achieving those goals and objectives, a description of IA programs, projects and initiatives that will result in the capabilities needed, and an IA risk management plan. The Navy IA Master Plan and updates as required will be submitted to CNO (N643) for approval and issuance.

(c) Submit Program Objectives Memorandum (POM) requirements to support IA programs as delineated in the Navy IA Master Plan.

(d) Execute Navy IA programs as defined in the Navy IA Master Plan.

(e) As the technical lead for Navy IA, provide systems and security engineering and integration testing and support for Navy information systems and networks with IA requirements. Provide input, review, and recommended updates to IA Publications. Establish and execute capability to provide on-site assessments to Navy commands, including vulnerability assessments coordinated by FIWC.

(f) Maintain a Navy IA research and development program to meet Navy requirements in accordance with the Non-Acquisition Program Decision Document (NAPDD) and as delineated in the Navy IA Master Plan. Coordinate IA R&D activities with the Office of Naval Research to ensure maximum and smooth transition of new technologies to operating forces, fully integrated for maximum cost effectiveness with existing technologies.

(g) As the Navy’s Certification Authority:

1. Provide high-level oversight and standardization for the system certification and accreditation process for all Service, Joint, development and acquisition programs across Navy.

2. Advise program managers and DAAs in their responsibility to assign a capable Certification Agent responsible for completing the certification and accreditation process in accordance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP), reference (f).

3. Establish and maintain a master file of Navy accredited systems and major network operations centers (NOCs). Ensure supporting certification and accreditation documents are analyzed for lessons learned, identification of system deficiencies and for incorporation in process improvements and the Navy IA Master Plan.

(h) Develop and centrally acquire Navy standard and specified IA products. Provide life cycle management support for centrally procured IA products and systems, to include operations and maintenance funding.

(i) Maintain the Navy INFOSEC Web Site and IA Help Desk as directed by CNO (N643).

1. Navy INFOSEC Web Site. The Navy INFOSEC Web Site on the World Wide Web provides access to the Navy IA Publications, as well as other IA related references, advisories and announcements, and a variety of resources on IA issues across Navy, the Department of Defense and other services and agencies. The INFOSEC Web Site URL on the Non-classified Internet Protocol Router Network (NIPRNET) is http://infosec.navy.mil/. On the Secret Internet Protocol Router Network (SIPRNET) the URL is http://infosec.navy.smil.mil/.

2. Information Assurance Help Desk. For routine technical and engineering assistance, an IA Help Desk has been established under COMSPAWARSYSCOM (PMW-161) to support Navy and Marine Corps commands on IA matters and provide guidance on specific questions for securing and certifying systems. The Help Desk is available at 1-800-304-4636.

(j) Support Navy Computer Network Defense by providing network analysis and management tools to support the Navy Component Task Force – Computer Network Defense (NCTF-CND) mission.

(4) COMSPAWARSYSCOM (PMW-162) shall conduct IA Vulnerability Assessments in support of the DITSCAP Certification and Accreditation process for developing systems.

(5) Commanders of Systems Commands and other Navy development and acquisition activities shall ensure Program Managers integrate information assurance requirements in the design of information systems and that all systems are delivered to naval customers with certification documentation to support accreditation requirements of ref (f).

(6) Commander, Naval Security Group Command (COMNAVSECGRU) shall:

(a) Serve as DAA for accreditation of Cryptologic systems and networks. Coordinate the Navy Service Cryptologic Element (SCE) program with the National Security Agency (NSA).

(b) Serve as DAA for SCI physical facilities under COMNAVSECGRU cognizance.

(c) Provide support, as coordinated by FIWC, in the conduct of vulnerability assessments and Red and Blue Team operations.

(7) The Communications, Information Systems, and Networks (CISN) Training Working Group, established under reference (g), shall:

(a) Identify Navy IA billet and training requirements.

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

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

(8) Chief of Naval Education and Training (CNET) shall:

(a) Develop Navy schoolhouse IA training and education.

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

(9) Fleet Information Warfare Center (FIWC) shall:

(a) Manage the Naval Computer Incident Response Team (NAVCIRT) for Navy; The NAVCIRT, located at FIWC, serves as the Navy primary computer incident response capability to provide assistance in identifying, assessing, containing, and countering incidents that threaten Navy information systems and networks. On request NAVCIRT will offer hands-on assistance to selected naval activities, such as deployed ships, that are under cyber-attack. FIWC will collaborate and 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.

(b) Provide CNO (N64) with monthly, quarterly, and annual summaries of reported Navy computer incidents.

(c) Provide timely advisories of newly identified vulnerabilities.

(d) Conduct on-line surveys for fielded systems.

(e) Provide vulnerability assessments and Red and Blue Team operations to requesting commands. Coordinate resources provided by COMNAVSECGRU and COMSPAWARSYSCOM PMW-161 as required.

(f) Provide intrusion detection monitoring, on-line surveys, and activity analysis and assessment in support of the NCTF-CND (see item 13).

(10) Director, Office of Naval Intelligence (ONI) shall:

(a) Coordinate Navy IA requirements for the Navy SCI/Intelligence program and the Navy portion of the DoD Intelligence Information System (DODIIS) with the Defense Intelligence Agency (DIA).

(b) Serve as DAA for Navy SCI systems.

(c) Assist CNO (N643) and COMSPAWARSYSCOM (PMW-161) by gathering relevant threat information to assist in defining system security requirements.

(d) Provide all-source, fused intelligence support to the NCTF-CND (see item 13).

(11) Commander, Naval Computer and Telecommunications Command (NCTC) shall:

(a) 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.

(b) As required, provide Internet web-hosting and demilitarized zone (DMZ) services for afloat units and small shore commands. A DMZ is a dedicated network segment that is used to separate public services from internal services.

(c) Ensure shore-based infrastructure solutions incorporate appropriate IA safeguards.

(d) Provide network operations, including monitoring and restoral functions in support of the NCTF-CND (see item 13).

(12) Director, COMSEC Material System (DCMS) shall:

(a) Maintain Central Office of Record (COR), ensuring the proper storage, distribution, inventory, accounting, and overall safeguarding of COMSEC materials for the Navy, Marine Corps, and Coast Guard, Military Sealift Command, and joint and allied commands, as required.

(b) Maintain the IA Publication Library as directed by CNO (N643).

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

(d) Under CNO (N643) direction, issue, publish and distribute guidance necessary to ensure National level (e.g., NSA) policies are followed and enforced.

(e) Act as the Navy High Assurance (Class 4) PKI Certificate Approving Authority. Communications Security (COMSEC) Material Issuing Office (CMIO) Norfolk provides a Navy Centralized CAW Facility (NCCF) to support DMS for other than Organizational Messaging and non-DMS FORTEZZA® requirements.

(f) Act as Navy Registration Authority for Medium Assurance (Class 3) PKI.

(13) Navy Component Task Force – Computer Network Defense (NCTF-CND) shall:

(a) Coordinate the defense of Navy computer networks and systems as directed by the Commander, Joint Task Force for Computer Network Defense (JTF-CND).

(b) Defend computer networks and systems within the Navy's elements of the Defense Information Infrastructure, as directed by the JTF-CND.

(c) When tasked, be responsible for the monitoring, restoral, and security of Navy networks.

(d) Monitor the Navy's Information Assurance Vulnerability Alert (IAVA) compliance and act as the Navy's Reporting Agent for IAVA.

(e) Coordinate/direct appropriate actions to ensure Navy web pages resident on the World Wide Web are in compliance with prescribed Department of Defense and Navy guidance.

(f) Make Information Operations Condition (INFOCON) recommendations to the Navy Command Center in response to a Computer Network Attack and report the Navy INFOCON status.

(14) Naval Criminal Investigative Service (NCIS) shall provide law enforcement and counter-intelligence support to the NCTF-CND and FIWC.

b. Individual Responsibilities

(1) Fleet Commanders-in-Chief and Second Echelon Commanders are responsible for implementation of the Navy IA Program within their respective claimancies and areas of responsibility and shall:

(a) Appoint in writing an Information Assurance Officer to oversee and provide IA guidance to subordinate organizations.

(b) Appoint in writing an Information Systems Security Manager (ISSM) to oversee and implement the IA program within the claimancy. This may be, but need not be the same individual assigned as Information Assurance Officer.

(c) 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 Publication Library.

(d) Request vulnerability assessment assistance and Red and Blue Team operations from FIWC to validate IA controls and practices.

(2) Commanding officers, commanders, and officers-in-charge are responsible for the overall management of IA at the command level and shall:

(a) Ensure all automated information systems or networks used by the command are individually and collectively accredited by the site DAA, or by the appropriate DAA in the case of information system services centrally procured or provided by another command.

(b) Ensure that all of the requisite safeguards, as documented in the respective System Security Authorization Agreement (SSAA), are implemented and that the site maintains accreditation. Assess the need to reaccredit with each system configuration change. While it is expected that the commander will be assisted in this effort by a certification agent, ISSM or Information System Security Officer (ISSO), accreditation is considered a command responsibility.

(c) Appoint, in writing, an ISSM. Where management and administrative functions have been consolidated within a Navy organization, the higher-level organization head may designate a single ISSM to manage IA for the entire organization, and subordinate ISSMs need not be appointed.

(d) Ensure that an ISSO is designated, as appropriate, for each information system and network in the organization, responsible for implementing and maintaining the site's information system and network security requirements. For smaller commands, the same individual may perform ISSM and ISSO duties.

(e) Ensure current standard operating procedures; inclusive of IA practices and procedures, are available and used for all information technology resources.

(f) Ensure IA awareness indoctrination and annual IA refresher training are conducted down to the user level, tailored to specific site requirements.

(g) Ensure all personnel performing IA functions receive initial basic and system specific training, required certification, as well as annual recurring, refresher, or follow-on training.

(h) Ensure any computer intrusion incident, or suspicion of one, is reported to FIWC at navcirt@fiwc.navy.mil or 1-888-NAVCIRT, as required by reference (i).

(3) Designated Approving Authority (DAA). General guidance on DAA roles and responsibilities is available in ref (h). Whether fulfilling the duties as DAA for program or systems development or as a site DAA, all DAAs shall:

(a) Ensure sites and systems under their cognizance are accredited in accordance with the DITSCAP (reference (f)). In doing so they shall review certification documentation to evaluate and determine an acceptable level of risk for information systems and for overall site configuration, to include the aggregate of information technology resources employed in a given geographic locale.

(b) Ensure accredited sites and systems maintain the approved security posture throughout the life cycle.

(c) Ensure the respective SSAA delineates the applicable IA training requirements for users, operators, maintainers, administrators, and managers in accordance with this instruction and all specified references. Site DAAs shall ensure the training requirements delineated in the SSAA are met and that training requirements for specific roles (e.g., DAA, ISSM, ISSO) are met prior to appointment.

(d) Coordinate any requirements for delegation of DAA authority with CNO (N643).

10. Action. All action addressees shall implement the guidance contained herein and all associated references to include the Navy IA Publication Library. 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.

R. W. MAYO
Rear Admiral, U.S. Navy
Director,
Space, Information Warfare,
Command and Control (N6)

Distribution:
SNDL Parts 1 and 2

LIST OF ACRONYMS

AIS:	Automated Information System
ASN:	Assistant Secretary of the Navy
C&A:	Certification and Accreditation
CIO:	Chief Information Officer
COMSEC:	Communications Security
COR:	Central Office of Record
DAA:	Designated Approving Authority
DASN:	Deputy Assistant Secretary of the Navy
DCMS:	Director, COMSEC Material System
DIA:	Defense Intelligence Agency
DII:	Defense Information Infrastructure
DITSCAP	Defense Information Technology Security C&A Program
DoD:	Department of Defense
DoN:	Department of the Navy
FIWC:	Fleet Information Warfare Center
FLTCINC:	Fleet Commander-in-Chief
GENSER:	General Services
IA:	Information Assurance
IAAV:	Information Assurance and Assist Visit
INFOSEC:	Information Systems Security
ISSM:	Information Systems Security Manager
ISSO:	Information Systems Security Officer
NAVCIRT:	Naval Computer Incident Response Team
NIPRNET:	Non-classified Internet Protocol Router Network
NISPOM:	National Industrial Security Program Operating Manual
NOC:	Network Operations Center
OLS:	On-line Survey
ONI:	Office of Naval Intelligence
PKI:	Public Key Infrastructure
RD&A:	Research, Development and Acquisition
SABI:	Secret and Below Interoperability
SBU:	Sensitive but Unclassified
SCE:	Service Cryptologic Element
SCI:	Sensitive Compartmented Information
SIOP:	Single Integrated Operations Plan
SIPRNET:	Secret Internet Protocol Router Network
SISSM:	Senior Information Systems Security Manager
SPAWAR:	Space and Naval Warfare Systems Command
SSAA:	System Security Authorization Agreement
URL:	Universal Resource Locator