



DEPARTMENT OF THE NAVY

NAVAL SEA SYSTEMS COMMAND
2531 JEFFERSON DAVIS HWY
ARLINGTON VA 22242-5160

IN REPLY REFER TO

NAVSEAINST 5239.2
Ser 00IT/010
29 Jul 98

NAVSEA INSTRUCTION 5239.2

From: Commander, Naval Sea Systems Command

Subj: INFORMATION SYSTEMS SECURITY

Ref: (a) P.L. 100-235 of 8 Jan 88, Computer Security Act of '87
(b) SECNAVINST 5239.3. (CH-1 of 15 Jan 97)
(c) DOD 5220.22-M of Jan 95
(d) NSTISSI No. 4009 of Aug 97
(e) NAVSO P-5239-15 of Jan 95
(f) NAVSEAINST 2300.1

Encl: (1) Minimum Protection Requirements for Unclassified and Sensitive Information

1. Purpose. The purpose of this instruction is to provide the basic policy and guidelines necessary for consistent and effective application of resources in ensuring the security and privacy of NAVSEA systems/information under the Computer Security Act of 1987 (references (a) and (b)).

2. Cancellation. NAVSEAINST 5239.1 of 29 November 1988 is canceled.

3. Scope. This instruction applies to information systems and networks operated by all NAVSEA activities and associated Program Executive Offices (PEO) that enter, process, store, or transmit unclassified, sensitive or classified information. This instruction and reference (c) also applies to contractors supporting NAVSEA or PEO activities and contractor owned facilities operating under NAVSEA/PEO authority. This instruction encompasses all information systems (IS) and networks that are procured, developed, modified, operated, maintained, or managed for NAVSEA organizational elements. To promote the use of standardized terminology and reduced documentation, the definition of terms as stated in reference (d) shall be applied in this instruction, unless otherwise specified.

4. Objectives

a. To properly apply Information Systems Security (INFOSEC) policies and procedures as a major component of the efforts to defend and protect NAVSEA information and information systems.

NAVSEAINST 5239.2
29 Jul 98

b. To integrate the technical and management processes of the various security disciplines Communications Security (COMSEC) and Computer Security (COMPUSEC) into a cohesive INFOSEC program.

c. To establish and implement programs for the certification and accreditation of information systems under NAVSEA control.

d. To incorporate a life cycle management approach to implementing INFOSEC requirements.

5. Precedence. Policy and requirements set forth by higher authority take precedence over the policy established in this instruction, except where it is more restrictive in this instruction.

6. Policy

a. All NAVSEA information and resources shall be appropriately safeguarded at all times with respect to 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. Safeguarding information technology resources and information shall be accomplished through the employment of defensive layers that include the INFOSEC disciplines, as well as sound administrative practices that include budgeting, funding, and executing the actions necessary to protect all IS resources.

b. All applications/programs will have a Controlled Access Protection (CAP) assessment conducted and submitted to the NAVSEA Waiver Approving Authority (WAA), through the applicable Designated Approving Authority (DAA), prior to implementation, in accordance with reference (e).

c. A program to audit the implementation of this instruction will be developed.

d. Copyrighted software will not be reproduced within NAVSEA, except as authorized within existing legal requirements. Personal accountability shall be enforced for all violations of copyright laws or licensing agreements.

29 Jul 98

e. Internet, Intranet and e-mail services shall be used in accordance with reference (f).

f. The use of privately owned hardware and software is prohibited unless approved by the requester's immediate supervisor and the organization/activity Information Systems Security Manager (ISSM). The processing of sensitive and classified information on privately owned resources is prohibited.

g. The DOD warning banner shall be installed and displayed to the user upon login so that it is clear that the system or computer is subject to monitoring and shall require an affirmative response by the user.

h. Information systems and networks will be certified and accredited to ensure that the appropriate technical and non-technical security features have been incorporated into the design and implementation.

7. Action

a. All NAVSEA/PEO activities shall:

(1) Utilize the Naval Sea Systems Command Information Systems Security Guidance Manual, S0300-CA-GYD-010, which contains the details to carry out this policy.

(2) Establish and implement security mechanisms and procedures to ensure that information entered, processed, stored, or transmitted by NAVSEA/PEO information systems is adequately protected with respect to confidentiality, integrity, availability, and privacy as shown in enclosure (1).

(3) Ensure that physical security measures are appropriate to protect NAVSEA/PEO information and resources.

(4) Network security firewalls to protect and prevent unauthorized access to NAVSEA/PEO information systems are required. Waivers to this requirement are to be submitted to the NAVSEA CIO, and are to include the results of an on-line survey conducted by the Fleet Information Warfare Center (FIWC). Waivers to implementing firewall protection must be approved in writing by the ISSM, DAA, and Commander/Commanding Officer of the organization. Firewalls are to be managed by the organization's ISSM.

NAVSEAINST 5239.2
29 Jul 98

(5) Monitor, detect, isolate and react to intrusions that could impact system and/or mission accomplishments.

(6) Implement procedures for reporting identified and/or suspected information system security violations.

(7) Develop and implement local policy and procedures to support effective employment of anti-virus software. The DoD licensed anti-virus software should be used where it is feasible.

(8) Develop a DAA approved connection process for remote access to NAVSEA systems and networks based on user needs.

(9) Develop policy whereby information on NAVSEA/PEO Internets and Intranets is reviewed and approved by appropriate authorities prior to posting. This policy is to ensure that all information will be protected commensurate with the sensitivity level of the information.

(10) Provide annual security awareness training for all personnel involved in the management, use and/or operation of NAVSEA information systems. Training shall be tailored to the responsibilities of the position.

(11) Ensure all NAVSEA/PEO information systems are accredited for operation at least once every three years or when changes occur that affect the security posture of the system. This can be accomplished for each system, group of systems and/or configuration.

(12) Develop and maintain an Information Systems Security Plan (ISSP) for each information system or group of systems. The DAA will determine whether an individual, group or activity ISSP is developed.

(13) Maintain an Information Systems Accreditation Schedule (ISAS).

(14) Develop contingency plans for systems and network servers that provide support across organizational entities as determined by the DAA. Plans shall be tested as appropriate.

(15) Develop procedures to ensure that electronic data and files are marked to reflect the appropriate classification or sensitivity. Procedures shall include provisions for handling and

29 Jul 98

destruction. At a minimum, all electronic information in the form of documents, images, or other human-viewable format, regardless of location, shall include plain-text markings indicating classification or sensitivity, as would be required if they were hardcopy products.

b. Individual Responsibilities:

(1) The NAVSEA Chief Information Officer (CIO) shall:

(a) Have oversight responsibility for the security of all Information Systems throughout the Naval Sea Systems Command and associated PEOs.

(b) Be the DAA for all Information Systems located in the NAVSEA Headquarters Campus. The NAVSEA CIO may designate specific persons who have the knowledge and authority to carry out the duties of the DAA from Directorates or PEOs for specific sections of the information systems their organizations have direct control over. The responsibility of the DAA may not be further delegated. No individual other than the Directorate/PEO Flag or SES may act for the Delegated DAA in their absence without the prior approval of the NAVSEA CIO.

(c) Appoint in writing the Command ISSM (CISSM) for NAVSEA.

(2) The Deputy Commander for Nuclear Propulsion (SEA 08), who is also the Deputy Assistant Secretary for Naval Reactors within the Department of Energy, shall implement all policy and practices pertaining to this instruction under his cognizance. The Deputy Director Naval Nuclear Propulsion Program shall 1) designate a DAA for the Naval Nuclear Propulsion Program, 2) designate a Naval Nuclear Propulsion Program ISSM and 3) have oversight responsibility for the security of all Information Systems throughout the Naval Nuclear Propulsion Program.

(3) Program Managers shall:

(a) Exercise the appropriate life cycle management practices to ensure their programs receive the proper INFOSEC certification.

NAVSEAINST 5239.2
29 Jul 98

(b) Forward all certification documentation for review and approval to the CISSM and/or appointed program technical staff. Documentation shall include a CAP assessment conducted in accordance with reference (e). All certifications will be approved by the appropriate DAA.

(4) The Commanders/Commanding Officers of NAVSEA Field Activities shall:

(a) Act as the DAAs for their activities. These responsibilities may be delegated in writing to a single member of the organization who has the knowledge and authority to carry out the duties of the DAA. This responsibility will not be delegated to the person responsible for daily management of information resources, unless the NAVSEA CIO approves a waiver. The responsibility of the DAA may not be further delegated. No individual other than the Commander/Commanding Officer may act for the DAA in their absence without the prior approval of the NAVSEA CIO.

(5) DAAs shall:

(a) Review certification/accreditation documentation to evaluate and determine 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 their life cycle.

(c) Appoint in writing, an ISSM for their respective command authority area.

(6) The CISSM shall:

(a) Be responsible for implementing this instruction, by preparing NAVSEA-wide INFOSEC plans, policies, and guidelines.

(b) Act as the focal point for all INFOSEC issues affecting NAVSEA and its field activities.

(c) Serve as the NAVSEASYSCOM Headquarters ISSM.

(7) ISSMs shall:

(a) Serve as the focal point and principal advisor for information systems security matters on behalf of the Commander/Commanding Officer.

(b) Appoint as required, an Information Systems Security Officer (ISSO) for each information system or group of information systems to maintain the security posture of that system. A Network Security Officer (NSO) may also be appointed to implement and maintain an organization's information systems and network security requirements.

(c) Manage the sites Internet security firewall where applicable.

8. Point of Contact. The NAVSEA point of contact for this instruction is the NAVSEA CISSM, Mr. Marc Apter, SEA 04IT3, 703-602-0336 x300, DSN 332-0336, fax number 703-602-8744, e-mail address: apter_marc@hq.navsea.navy.mil.


G. P. NANOS, JR.

NAVSEAINST 5239.2
29 Jul 98

Distribution:
NAVSEA Special List Y1
PEO DD21
PEO CV

SNDL C84 COMNAVSEASYSKOM Shore Based Detachments (less 84J)
C84B COMNAVSEASYSKOM Detachments
FKP COMNAVSEASYSKOM Shore Activities (less FKP6B & FKP24)
A1J1K PEO USW
A1J1L PEO TAD/SC
A1J1M PEO MIW
A1J1N PEO SUB
A1J1P PEO EXW
C21 AA UNSECNAVDET
FT88 EDOSCOL

Copy to:
Defense Printing Detachment
1401 South Fern St
Arlington, VA 22202-2889

Stocked: SEA 09A1 (5 copies)

Minimum Protection Requirements for Unclassified and Sensitive Unclassified Information

Categories of Information	Review Process	Encryption Method	Protection of Static Information Files		Protection of Dynamic Information Transmission	
			Encryption Method	Campus Network	Off-Campus Network	
Public Release Information	PAO, Contract or FOIA Release	N/A	None	None	None	None
Unclassified NINPI	Dir/CMD DAA & SEA 08 Release	NSA Approved (NES, Fortezza, STU III) & NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID Password/*	Secure User ID Password/Encrypt	
Internal Personnel Rules and Practices	Dir/CMD DAA & FOIA Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID/Password/*	Secure User ID/Password/Encrypt	
-Operating Rules, Guidelines, & Manuals for investigators, inspectors, auditors, or examiners; release of which would enable circumvention of statutes, regulations, executive orders, manuals, directives, and/or instructions	Dir/CMD DAA, Security & FOIA Release	N/A	User ID/Password	User ID/Password	User ID/Password	
-Examinations questions and answers used to determine qualifications	Dir/CMD DAA & FOIA Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID/Password/*	Secure User ID/Password/Encrypt	
-Computer Software, release of which would enable circumvention of statute or DON rules, regulations, orders, manuals, directives, or instructions	Dir/CMD DAA & FOIA Release	N/A	User ID/Password	User ID/Password	User ID/Password	
-Security Classification Guides	Dir/CMD DAA & FOIA Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID/Password/*	Secure User ID/Password/Encrypt	
Statute That Specifically Prohibits Release and Permits no Discretionary Release	Dir/CMD DAA Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID Password/*	Secure User ID Password/Encrypt	
-NSA Information, P.L. 86-36, Sect 6	Dir/CMD DAA & NSA Release	NSA Approved (NES, Fortezza, STU III)	Secure User ID/Password/*	Secure User ID Password/Encrypt	Secure User ID Password/Encrypt	
-Patent Secrecy, 35U.S.C. 181-185 (Patent on Gov't hold)	Dir/CMD DAA & Legal Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID Password/*	Secure User ID Password/Encrypt	
-(Declassified) Restricted Data & Formerly Restricted Data, 42 U.S.C. 2162	Dir/CMD DAA & Security Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID Password/*	Secure User ID Password/Encrypt	
-Communication Intelligence, 18 U.S.C. 798	Dir/CMD DAA & Security Release	NSA Approved (NES, Fortezza, STU III)	Secure User ID/Password/*	Secure User ID Password/Encrypt	Secure User ID Password/Encrypt	
-Authority to Withhold from Public Disclosure Certain Technical Data, 10 U.S.C. 130 (Critical Technology/Export Controlled)	Dir/CMD DAA & Security Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID Password/*	Secure User ID Password/Encrypt	
-Protection of Procurement related Proprietary & Source Selection Information during the period of the Procurement Process, 10 U.S.C. 130	Dir/CMD DAA & Contracts Release	NIST FIPS 140-1 Compliant	Secure User ID/Password/*	Secure User ID Password/*	Secure User ID Password/Encrypt	

Minimum Protection Requirements for Unclassified and Sensitive Unclassified Information

-Protection of other information exempted from release by statute; see you local FOIA Representative for a list of applicable information statutes	Dir/CMD DAA Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID/Password/*	User ID/Password/Encrypt
Trade Secrets or Commercial or Financial Information	Dir/CMD DAA & Contracts Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID Password/*	User ID/Password/Encrypt
-Computer software which is Copyrighted under the Copyright Act of 1976, the disclosure of which would have an adverse impact on the potential market value of a copyrighted work	Dir/CMD DAA, FOIA & Contracts Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID Password/*	User ID/Password/Encrypt
-Trade Secrets/Proprietary Information, etc.	Dir/CMD DAA, FOIA & Contracts Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID Password/*	User ID/Password/Encrypt
-Prep Docs for Admin Proceedings or Litigation	Dir/CMD DAA, FOIA & Legal Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID Password/*	User ID/Password/Encrypt
-Inspection, Audit, Investigation, etc. Reports	Dir/CMD DAA, FOIA & IG Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID Password/*	User ID/Password/Encrypt
Personal info such as date/place of birth, home address & telephone number, medical info, family status, investments, performance evals, SSN, disciplinary info, allegations of wrongdoing, that if disclosed are an Unwarranted Invasion of Personal Privacy	Dir/CMD DAA, FOIA & Personnel Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID/Password/*	User ID/Password/Encrypt
Records or Information Compiled for Law Enforcement Purposes	Dir/CMD DAA, FOIA & Security Release	NIST FIPS 140-1 Compliant	User ID/Password/*	User ID Password/*	User ID/Password/Encrypt
D/C DAA Release - Directorate/Command DAA Release					
* - Encryption is required where physical security is inadequate for the sensitivity of the information					
User ID/PW - User Identification & PassWord; A unique identification for each user, and a password meeting current policy					
Secure User ID/PW - Secure User Identification & PassWord; Utilization of the Fortezza Card for Identification & Authentication (I&A), or the use of other hardware or software approved by the NAVSEA DAA (e.g. The Secure-ID Card used by the Shipyards)					
CAMPUS INTRANET - Networks (LAN & WAN) directly (physically) controlled by the local NAVSEA Organization					