

CH-1 entered 26 May 99

NAVSUBSCOLINST 5239.2C

01E

30 Jul 98

NAVSUBSCOL INSTRUCTION 5239.2C

SUBJ: INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM

Ref: (a) SECNAVINST 5231.1C
(b) SECNAVINST 5239.3
(c) OPNAVINST 5239.1A
(d) CNETINST 5231.1B
(e) NAVSO P-5239-15
(f) NAVSUBSCOLINST 7321.1L

Encl: (1) INFOSEC Staff Organization
(2) Definition of Terms
(3) INFOSEC Survey
(4) IS Configuration Change Request
(5) Department IS LCM Report
(6) Department IS Acquisition Strategy Plan (ASP)
[Hardware]
(7) Department IS Acquisition Strategy Plan (ASP)
[Software]
(8) AIS Repair Request
(9) INFOSEC Incident Report
(10) INFOSEC Violation Report
(11) INFOSEC Non-Disclosure Agreement

1. Purpose

a. To establish the command Information Systems Security Program.

b. To define organizational structure that executes the INFOSEC Program.

c. To set forth policies and guidelines necessary for implementation of Department of the Navy INFOSEC Program throughout NAVSUBSCOL.

d. To apply basic policy and principles of INFOSEC as they relate to information technology (IT), since use of such systems introduces vulnerabilities uniquely attributable to that technology.

e. To establish processes to implement references (a) through (e).

f. To set policies and guidelines for use of the INTERNET.

2. Cancellation. NAVSUBSCOLINST 5239.2B

3. Objective. To ensure availability of reliable information

NAVSUBSCOLINST 5239.2C

30 Jul 98

and automated support required to meet the command's mission by adequately protecting all information systems against unauthorized disclosure, modification, destruction or denial of service, whether accidental or intentional.

4. Scope. This instruction applies to:

a. All Federal Information Processing (FIP) resources, embedded FIP resources, information systems (IS), automated information systems (AIS) and networks designed, developed or procured by NAVSUBSCOL.

b. All FIP resources, embedded FIP resources, IS, AIS and networks designed, developed or procured by other activities or contractors for use at NAVSUBSCOL.

c. Printing, imaging, recording or other equipment that are part of IS, connected to IS, or driven by process control or embedded computers.

5. Organization. Enclosure (1) illustrates the organizational structure of the Information Systems Security (INFOSEC) Staff. The Designated Approving Authority (DAA) appoints in writing a Security Officer, Communications Security (COMSEC) Material System (CMS) Custodian, TEMPEST Control Officer and Automated Information Systems (AIS) Security Officer. Appointments to other INFOSEC Staff positions are designated in writing by the Department Head. The AIS Security Officer reports to the Security Manager and Designated Approving Authority.

6. Roles and Responsibilities. Personnel assigned to the INFOSEC Staff must accomplish their duties as described in references (b) and (c), and this instruction. Since each department within the command maintains some autonomy, AIS Department Security Officers (AISDSO) shall be appointed by, and act for, the Department Head as the AIS Security Officer (AISSO) does for the DAA. However, AIS Department Security Officers also are responsible to the AIS Security Officer and shall be entered in the Command Collateral Duty list. Department representatives shall have at least one year remaining at the command prior to their projected rotation date.

7. Definitions. References (a) through (c) provide definitions and acronyms essential to understanding program concepts. Enclosure (2) contains additional definitions specific to NAVSUBSCOL.

8. Training. The AIS Security Officer will ensure all personnel who operate, manage or administrate IS receive training in accordance with references (b) and (c).

a. End Users. AIS Department Security Officers shall administer training to their departments' IS end users at least

30 Jul 98

annually. A copy of all related training reports must be submitted to the AIS Security Officer. End user training reports shall be retained by the AIS Security Officer for two years.

b. INFOSEC Staff. Members of the INFOSEC Staff must receive formal training within three months of appointment.

c. Upper-Level Managers includes, but not limited to Department Head, Division Heads, officers and civilians with equivalent positions. All upper-level managers shall receive formal training within six months of assignment.

9. Accreditation. IS shall be protected by continuous use of appropriate protective measures such that remaining risks are acceptable to the DAA. Accreditation only can be accomplished by a process of preparation, risk management and certification.

a. Preparation

(1) INFOSEC Survey. Enclosure (3) shall be used to collect information on IS for inclusion in the accreditation process. Survey will be completed by the responsible AIS System Security Officer, approved by the cognizant Department Head and returned to the AIS Security Officer. INFOSEC Surveys shall be completed in support of accreditation and to request a change in accreditation status. INFOSEC Surveys shall be verified at the direction of the AIS Security Officer; Department Head approval need be obtained only if verification results in a change of survey data.

(2) Configuration Control. IS configurations shall be monitored by the AIS Security Officer. Each system and terminal must be comprised of the internal hardware, external equipment and software specified in the IS configuration report. Changes to an IS configuration may be accomplished with AIS Security Officer approval of an IS Configuration Change Request, enclosure (4). An Inter-Departmental Transfer of Plant Account Minor Property, contained in reference (f), need not be completed when an IS Configuration Change Request is submitted. AIS System Security Officers are notified of approved configuration changes when a new configuration report is issued.

(3) Activity INFOSEC Plan. The AIS Security Officer shall submit an Activity INFOSEC Plan to the DAA annually, or upon change. The Activity INFOSEC Plan shall include the elements for an Activity AIS Security Plan specified in reference (b), and be maintained current.

(a) IS Accreditation Schedule (AS). The AIS Security Officer shall maintain a current IS AS in accordance with reference (b). The IS AS shall be forwarded to the DAA for promulgation quarterly, independent of the Activity INFOSEC Plan.

30 Jul 98

(b) Interim Authority to Operate (IATO). When operational necessity dictates, the DAA may grant IATO for systems on the IS Accreditation Schedule. IATO shall not exceed one year. No system may operate unless granted accreditation or IATO by the DAA.

b. Risk Management. Accreditation groups shall be derived by the AIS Security Officer in support of risk management and accreditation group status. The AIS Security Officer assesses additional risks when introduced and initiates appropriate action with respect to accreditation. In instances where accreditation or IATO should be removed, the AIS Security Officer places the group on the accreditation schedule. Accreditation is considered by the DAA once the accreditation group has undergone risk analysis, contingency planning and testing, and security test evaluation.

(1) Risk Analysis. The AIS Security Officer shall determine the risk analysis method appropriate for each accreditation group. Upon completion of risk assessment, the AIS Security Officer will forward a report to the cognizant Department Head detailing the accreditation groups= security posture and recommendations for improvement. The Department Head then compares the costs and benefits for recommended security safeguards and implements those appropriate. Risk Analysis Reports are returned to the AIS Security Officer when the Department Head has completed his action.

(2) Contingency Plans. Mission critical IS shall have contingency plans developed and tested annually in accordance with references (b) and (c). The DAA determines which IS are mission essential and specifies required contingency plans in the Activity INFOSEC Plan. AIS Department Security Officers will develop, test and document all contingency plans.

(3) Security Test and Evaluation (ST&E). The AIS Security Officer shall determine the ST&E method appropriate for each accreditation group and appoint members of the INFOSEC Staff to prepare and conduct testing. The AIS Security Officer shall then assess results and document the evaluation in an ST&E Report.

c. Accreditation Documentation consists of the Risk Analysis Report, Contingency Plan(s) and testing documents, and the ST&E Report. Upon completion of the risk management phase, the AIS Security Officer may certify an accreditation group as having met the requirements of reference (b) and this instruction. Accreditation Documentation shall be forwarded to the DAA, via the cognizant Department Head, with a certification statement and the AIS Security Officer=s recommendations concerning accreditation.

d. Accreditation Statement. Following review of documentation in support of accreditation, the DAA may issue an

30 Jul 98

accreditation letter for the accreditation group, allow continued operation of systems within the group under an IATO, or restrict operations. The AIS Security Officer may include additional systems and terminals into an accreditation group at any time during the accreditation process provided the additions are consistent with the common architecture and operational environment of the group. Accreditation shall be reviewed by the AIS Security Officer in accordance with reference (b).

10. Life Cycle Management (LCM). Prior to purchasing information resources (IR), the Department Head shall plan and budget for each project. LCM documentation shall be submitted in accordance with references (a) and (d), via the AIS Security Officer and Supply/Fiscal Officer, for technical and funding certification. LCM documentation shall include Department IS LCM Reports, INFOSEC Surveys for proposed new systems and, when required, Mission Needs Statement (MNS), System Decision Paper (SDP) and Abbreviated System Decision Paper (ASDP).

a. Department IS LCM Report. Enclosure (5) shall be used to budget for the life cycle of each system. Department Heads shall ensure their IS LCM Report reflects accurate cost estimates and is submitted to the Commanding Officer by 1 September each year for approval.

b. Mission Needs Statement (MNS) is documented in accordance with references (a) and (d) by the cognizant AIS Department Security Officer.

c. Systems Decision Paper (SDP). The cognizant AIS Department Security Officer shall submit a current SDP at each LCM milestone in accordance with references (a) and (d).

d. Abbreviated Systems Decision Paper (ASDP). When allowed by references (a) and (d), cognizant AIS Department Security Officers will prepare an ASDP in lieu of MNS and SDP. Review and approval of ASDP shall be in accordance with reference (d) and this instruction.

e. Department IS Acquisition Strategy Plan (ASP). Department Head must plan specific IR purchases for each quarter of an entire fiscal year. However, purchases will be authorized for only the first three quarters. Enclosures (6) and (7) shall document the department's IR purchase requests by system and terminal number. Spending for each system on the IS ASP shall be consistent with the system's estimated cost in the Department IS LCM Report. Further, ASP must be supported by LCM documentation in accordance with references (a) and (d). Department Heads shall submit their IS ASP to the Commanding Officer by 1 September each year for approval, using enclosures (6) and (7).

11. IR Procurement. The AIS Security Officer shall ensure all IR procurement action has first met LCM requirements. Purchases may include new operating IS and planned upgrades or repairs of

NAVSUBSCOLINST 5239.2C
30 Jul 98
existing resources.

a. New Systems and Upgrades

(1) Requisitions are prepared for items listed in an approved IS ASP by the cognizant Repair Parts Petty Officer (RPPO). IR requisitions shall be submitted to the Supply/Fiscal Officer via the AIS Security Officer. The AIS Security Officer ensures the requisition is prepared correctly for the item(s) under procurement and is supported by LCM documentation. The Supply/Fiscal Officer shall coordinate any special funding requirements, monitor the progress of all purchases, and provide copies of all requisitions, contracts and modification documents to the ASP Security Officer.

(2) Accreditation. The AIS Security Officer will assign system and terminal numbers, revise Configuration Database(s), and initiate the accreditation process, as required. The AIS System Security Officer shall submit an approved INFOSEC Survey, enclosure (3), to the AIS Security Officer prior to operating a new information system.

b. Repair. An AIS Repair Request, enclosure (8), shall be used to notify the AIS Security Officer of any IS related equipment needing repair or replacement. The AIS Security Officer evaluates all repair requests and directs corrective action. Requisitions are prepared and processed the same as upgrades, except items need not be specified in an IS ASP. Procurement of repair or replacement items shall be accomplished within thirty days of repair evaluation. If repair costs exceed that specified for the system, LCM documents need not be revised until the following fiscal year.

12. IR Distribution. The AIS Security Officer is the point of contact for IR regardless of origin. IR received by departments

other than supply must be reported to the AIS Security Officer, accounted for in LCM documentation, and be included in the accreditation process. The receiving agency shall be the Supply Department for procurement of IR.

a. Receipt. The Supply/Fiscal Officer shall ensure all warrantee and registration material is removed from received IR and forwarded to the AIS Security Officer for action. A copy of all active materials must be maintained on file by the AIS Security Officer.

b. Deployment. The AIS Security Officer shall provide a copy of new configuration reports to the AIS System Security Officer when IR is issued. Before installation onto a system or terminal, the AIS System Security Officer must ensure the IR is assigned to its configuration. Additionally, the AIS System Security Officer must verify the system has been granted IATO or accreditation by the DAA prior to operation.

(1) Hardware. Before issuing hardware to the cognizant RPPO, the Supply/Fiscal Officer will provide the AIS Security Officer information required for configuration control. Further, all original software media associated with hardware shall be removed and forwarded to the AIS Security Officer before deployment. IS external hardware must be recorded in plant account. The cognizant Department Head is responsible for ensuring such equipment is processed appropriately in accordance with reference (f).

(2) Software. All software licensing agreements are enforced by the INFOSEC Staff. The AIS Security Officer monitors license use in configuration control. Media containing software shall **not** be entered into plant account since the intrinsic value of software is in the license. The AIS Security Officer shall maintain control of all original licenses, copyrighted, public domain and evaluation software media. A member of the receiving department=s INFOSEC Staff must provide the correct media and produce a working copy of software for installation. Working copies of software shall be safeguarded as if the media were originals.

c. Inoperative, Excess and Obsolete IR. IR identified as in excess or obsolete shall be placed into the department=s pool of available assets. Inoperative equipment shall be evaluated for repair and placed into the pool. When the AIS Department Security Officer has determined the IR is not desired by the command, the material shall be surveyed per reference (f), if required, and transferred in accordance with DOD Directive 7950.1.

13. IS Operation. IS operated in NAVSUBSCOL spaces shall be used for official government business only. Any other use constitutes noncompliance with the Computer Security Act of 1987, Code of Conduct (military) and Standards of Conduct (civilian). Additionally, each system must be granted IATO or accreditation by the DAA prior to operation in accordance with references (b) and (c). All IS shall operate in Dedicated Mode per reference (e) unless otherwise specified in the Activity INFOSEC Plan.

a. Privately Owned Assets. Use of privately owned or leased IR within NAVSUBSCOL spaces requires written authorization from the Commanding Officer. Such permission shall be granted only for performance of official government business. These assets must be accredited and regulated the same as those owned by NAVSUBSCOL. Privately owned or leased assets shall not be used to acquire, store, control, transmit or display classified data.

b. Department of Defense or Contractor Owned Assets. IR owned, operated or provided by a Department of Defense activity or contractor for use in NAVSUBSCOL spaces must be granted an IATO or accreditation by the DAA prior to operation, and are

NAVSUBSCOLINST 5239.2C

30 Jul 98

subject to the requirements of references (a) through (e) as well as this instruction. In cases where the activity or contractor fails to furnish an IATO or accreditation statement, the cognizant Department Head shall enter the assets into LCM documentation, specifying funding sources, and the AIS Security Officer will initiate the accreditation process. However, if the activity or contractor intends only temporary operation of unclassified IR, the cognizant Department Head need only obtain written authorization from the Commanding Officer to grant operation for the intended period of use. Under no circumstances shall this period exceed six months.

c. Communications. AIS System Security Officers must maintain terminal locator lists identifying NAVSUBSCOL systems that communicate with IR outside the command. The list shall specify what activities the system accesses and an inventory of other NAVSUBSCOL assets that also access the same resources. Classified communications shall be encrypted or be transmitted along a Protected Distribution System (PDS) in accordance with OPNAVINST C2200.13.

d. Malicious Code. Executable files shall be obtained only from the AIS Security Officer. No such files should be transmitted or acquired from an IR, nor be transferred on removable media unless authorized by the AIS Security Officer. Such files may include malicious code that could compromise exposed systems. Therefore, the AIS Security Officer must ensure that all executable files are scanned properly for malicious code prior to issue. Detection of malicious code shall be treated as an INFOSEC incident and reported to the AIS Security Officer.

e. INFOSEC Incidents and Violations. INFOSEC Incidents shall be reported to the AIS Security Officer with an INFOSEC Incident Report, enclosure (9). The AIS Security Officer will evaluate all incidents and report violations to the ISSM and Commanding Officer with an INFOSEC Violation Report, enclosure (10).

f. System Documentation. AIS System Security Officers are responsible for maintaining a system binder near each IS. Included in the binder shall be a security operating procedures, special procedures, contingency plans, terminal locator lists, applicable Memoranda Agreements, a current list of authorized users, most recent configuration reports provided by the AIS Security Officer and any other technical or functional documentation relevant to the system. The binder shall be used by end users to train on security procedures and serve as a source of information specific to the system. The AIS Security Officer promulgates separately, and issue changes to SOP. AIS System Security Officers may require additional security or operational measures in the form of special procedures.

14. Action

a. Security Officer shall coordinate and monitor Computer Security (COMPUSEC), Communications Security (COMSEC) and Emanations Security (TEMPEST) within NAVSUBSCOL.

b. CMS Custodian shall enforce, coordinate and monitor telecommunications security to include transmissions, emissions, use of cryptographic devices and physical security of COMSEC material and NAVSUBSCOL.

c. TEMPEST Control Officer shall enforce, coordinate and monitor emanations security to include control of compromising emanations from telecommunications and information resources at NAVSUBSCOL.

d. AIS Security Officer shall:

(1) Provide training to INFOSEC Staff and upper-level management in accordance with reference (c) and this instruction.

(2) Enforce, coordinate and monitor accreditation process in accordance with references (b) and (c).

(3) Act as Certification Authority for all information systems in accordance with reference (b).

(4) Forward all documentation in support of accreditation to the Designated Approving Authority with recommendations concerning accreditation.

(5) Report all INFOSEC Violations to the Security Manager and Designated Approving Authority.

(6) Develop and maintain current information systems security operating procedures.

(7) Enforce, coordinate and monitor life cycle management, for all information resources in accordance with references (a), (b) and (d).

(8) Review all information resource procurement for compliance with references (a), (b) and (d).

(9) Evaluate and direct AIS repair action.

(10) Monitor information resources distribution for inclusion into configuration control and the accreditation process.

(11) Enforce, coordinate and monitor implementation of

NAVSUBSCOLINST 5239.2C

30 Jul 98

references (a) through (e) as specified in this instruction.

e. Supply/Fiscal Officer shall:

(1) Review life cycle management and procurement documentation for compliance with references (a) and (d), and coordinate funding requirements.

(2) Provide the AIS Security Officer information required to monitor distribution of information resources.

f. Department Head shall:

(1) Appoint in writing an AIS Department Security Officer, AIS System Security Officers, Network Security Officers and Terminal Area Security Officers.

(2) Evaluate and manage information resources within their department to include approval of information resource procurement, along with changes in INFOSEC surveys.

(3) Assess INFOSEC risks and implement cost effective safeguards.

(4) Submit life cycle management documentation required by references (a), (b) and (d), and this instruction.

g. Department Repair Parts Petty Officer shall:

(1) Prepare all information resource requisition documents approved for procurement in life cycle management by the Commanding Officer.

(2) Prepare all information resource requisitions for AIS repairs/replacements.

(3) Advise their Department Head on matters concerning INFOSEC and life cycle management.

(4) Act as Program Manager for all department information system projects in accordance with references (a) and (b).

h. AIS Department Security Officers shall:

(1) Provide training for all information system end users within their department in accordance with references (b) and (c).

(2) Enforce, coordinate and monitor the accreditation process within their department in accordance with references (b) and (c), including development and testing of required contingency plans and participation in risk management.

(3) Advise their department Department Head on matters concerning INFOSEC and life cycle management.

(4) Act as Program Manager for all department information system projects in accordance with references (a) and (b).

i. AIS System Security Officers shall:

(1) Indoctrinate information systems end users in INFOSEC policy and requirements.

(2) Retain signed non-disclosure agreements required by reference (b).

(3) Enforce, coordinate and monitor accreditation process for information systems under their cognizance in accordance with references (b) and (c), including participation in risk management.

(4) Perform INFOSEC Surveys in support of accreditation, requested changes in accreditation status, and when directed by the AIS security Officer.

(5) Enforce configuration control as required by reference (b) and by this instruction.

(6) Verify information systems are granted Interim Authority to Operate or Accreditation prior to operation.

(7) Maintain system documentation as required by reference (b) and this instruction, including development and implementation of special procedures.

(8) Report all INFOSEC Incidents to the AIS Security Officer.

(9) Initiate AIS repairs, inform the AIS Security Officer, and advise procurement action.

j. Information Systems End Users shall:

(1) Understand and comply with references (b) and (c), this instruction, security operating procedures, and applicable special procedures.

(2) Sign a non-disclosure statement, enclosure (11) as required by reference (b), prior to accessing an information system.

(3) Inform the AIS Security Officer of practices dangerous to security, improper operations or needed repairs.

(4) Obtain permission from the AIS System Security Officer to change an IS configuration, location, functionality,

NAVSUBSCOLINST 5239.2C
30 Jul 98
architecture or environment.

15. INTERNET

a. Policy. This policy amplifies CNO message 212001Z Jul 95, Guidelines for Naval Use of the INTERNET, and is in accordance with the Guidelines established by Chief of Naval Education and Training (CNET).

(1) CNET shall provide Naval Submarine School with mission related access for INTERNET servers and services.

(2) The INTERSERVICE SUPPORT AGREEMENT (ISA) from Commanding Officer, Naval Education and Training Professional Development and Technology Center (NETPDTTC), details the support of automated data processing/automated services for the Local Area Network (LAN) and the INTERNET. All server systems will operate in an environment with FIREWALL mechanisms maintained at CNET.

b. RESPONSIBILITIES.

(1) The Commanding Officer of Naval Submarine School is the Designated Approving Authority for Information that will be accessed/provided via the INTERNET by personnel at NAVSUBSCOL.

(2) The Automated Information System Security Officer shall:

(a) Ensure that information provided on the command's World Wide Web (WWW) home page/s does not contain classified, unclassified sensitive, or privacy information, or information that could enable the recipient to infer classified or unclassified sensitive information, either from individual segments of the information, or from the aggregate of all the information available.

(b) Support, as requested the design and maintenance of NAVSUBSCOL World Wide Web (WWW) Home page for the NAVSUBSCOL Public Affairs Office.

(c) Ensure that official information cleared for public release is consistent with established DoN, DoD, and National policies and programs.

(d) Review, as required, all WWW Home page or other INTERNET information to ensure compliance.

(3) The Public Affairs Officer shall:

(a) Serve as the NAVSUBSCOL WEB administrator for WWW design and site maintenance as well as the proponent office for site servicing. The public affairs office address will serve as the E-mail address.

(b) Ensure the appropriateness and factual accuracy of all information. Ensure that official information cleared for public release is consistent with established DoN, DoD, and National policies and programs. Avoid links to vendors selling services and products to the government, as such a link might give the appearance of DoN endorsement of product or service, or showing favoritism to a particular vendor.

(c) Ensure that all material submitted for publication does not contain classified information, unclassified sensitive information, or privacy act information, or information that could enable the recipient to infer classified information or unclassified sensitive information, either from individual segments of the information or from the aggregate of all the information available.

c. USAGE. The INTERNET must be used with the highest professional standards and credibility of Naval Submarine School in mind.

(1) Only client/browser software provided by NETPDTC will be used for INTERNET access. No personal software will be used without approval from the Commanding Officer, Naval Submarine School. The use of dial-up modems to access the INTERNET is prohibited, such access by-passes FIREWALL protection.

(2) No public domain freeware software shall be downloaded from the INTERNET at NAVSUBSCOL without prior approval from the Automated Information System Security Officer and the Commanding Officer. All AIS rules concerning configuration control and notification apply to software approved for down load from the INTERNET.

(3) The use of the INTERNET for educational purposes, local/national news, sports scores, stock reports, and pertinent information is permitted as long as it does not conflict with work and is in keeping with professional standards and Navy Core Values.

NAVSUBSCOLINST 5239.2C
30 Jul 98

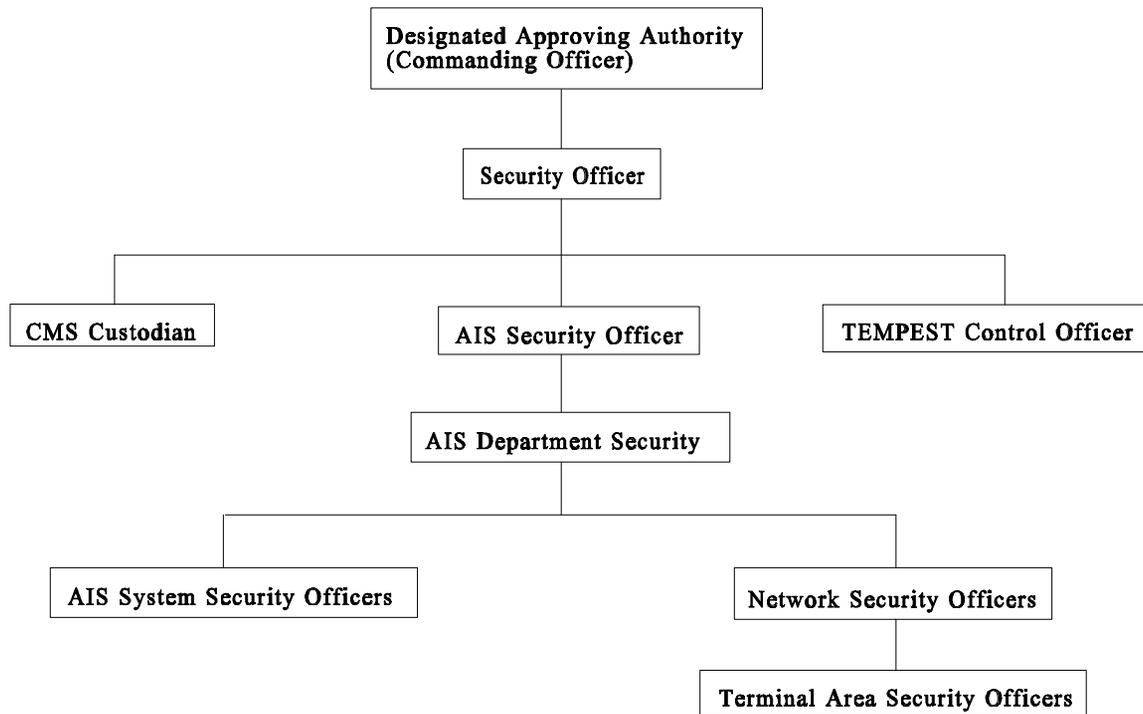
(4) Information placed on the INTERNET, for public access, must be submitted through the same public affairs channels as "hard" copy material proposed for publication, (for national release). All information must first be cleared through the NAVSUBSCOL Public Affairs Officer. These regulations apply: U.S. Navy Public Affairs Regulations, SECNAVINST 5720.44A; Department of the Navy Privacy Act Program, SECNAVINST 5211.5D;

and Department of the Navy Information and Personnel Security Program Regulation, OPNAVINST 5510.1H.

K. B. LEAHY

Distribution
Case A

INFOSEC STAFF ORGANIZATION



DEFINITION OF TERMS

INFOSEC INCIDENT: Any practice dangerous to INFOSEC or could result in an INFOSEC violation. *See also*, INFOSEC Violation.

INFOSEC VIOLATION: Any event that results in unauthorized disclosure, modification, destruction or denial of service, whether accidental or intentional, of information stored, processed or displayed by an information system.

SYSTEM: Hardware, firmware and software comprising a single stand-alone AIS or network of AIS. An AIS or network may communicate with other systems on a limited basis; however, system boundaries are defined by all AIS, networks and computer resources with extended periods of communication.

TERMINAL: Hardware, firmware and software comprising an otherwise single stand-alone AIS connected or communicating with other terminals or AIS a majority of operational time. Terminals may be AIS networked or input/output devices communicating with an AIS or network of AIS.

INFOSEC SURVEY

1. System Identification:

System Number:		Terminal Number:					
Accreditation Group:		Nomenclature:					
Mode of Operation:		Operating System:					
<input type="checkbox"/>	Desktop:	<input type="checkbox"/>	Stand-Alone	<input type="checkbox"/>	Network (LAN)	<input type="checkbox"/>	Government Owned
<input type="checkbox"/>	Mobile	<input type="checkbox"/>	Communications	<input type="checkbox"/>	Network (WAN)	<input type="checkbox"/>	Private/Contractor
Other (s) :							

2. Location:

Department:	Code:	Building:	Room:
-------------	-------	-----------	-------

3. System Function:

<input type="checkbox"/>	Graphics Presentations	<input type="checkbox"/>	Word Processing	<input type="checkbox"/>	Spread Sheet	<input type="checkbox"/>	Data Base Management	<input type="checkbox"/>	Project Management	<input type="checkbox"/>	Communications
Other (s) :											

4. System Environment:

<input type="checkbox"/>	Guard Force	<input type="checkbox"/>	Closed Circuit TV	<input type="checkbox"/>	Intrusion Detection System	<input type="checkbox"/>	Visitor Control	<input type="checkbox"/>	Escort Procedures	<input type="checkbox"/>	Badge Identification System
Other (s) :											

5. System Classification:

<input type="checkbox"/>	Unclassified	<input type="checkbox"/>	Sensitive Unclassified	<input type="checkbox"/>	Confidential	<input type="checkbox"/>	Secret	<input type="checkbox"/>	Top Secret
Other (s) :									

6. ADP System Security Officer:

DAA: <input type="checkbox"/> CO, NAVSUBSCOL <input type="checkbox"/> Other:			
Last Name	First Name	MI	Rank/Rate
Department	Code	Phone Extension	PRD/Loss Date

7. Approved:

Department Department Head Signature _____
Date

REQUEST IS CONFIGURATION CHANGE

From:	Department/Code Transferring Item (s)
To:	ADP Security Officer
Via:	Department Code Receiving Item (s)
Subj:	INFORMATION SYSTEMS CONFIGURATION CHANGE REQUEST

1. Request the following change (s) be made to IS configurations:

Plant Account Minor Property or Control Number	Nomenclature	Serial or License Number	Dollar Value
			\$

Transferring From					Receiving To				
Department	Division	System	Terminal	Bldg/Room	Department	Division	System	Terminal	Bldg/Room
Department/Division Head Transferring Item (s)					Department/Division Head Receiving Item (s)				
Signature				Date	Signature				Date
Remarks									

Distribution (Plant Account Minor Property Transfers Only):
 Plant Account Minor Property Administrator
 Plant Account Minor Property Responsible Officer, Transferring Code
 Plant Account Minor Property Responsible Officer, Receiving Code

INSTRUCTIONS

System Number: Specify number assigned to the IS by the AIS Security Officer and used in configuration control. If specifying a new system with no assigned number, write in a sequential letter (i.e., A, B, C...) .

Life Cycle (YRs) : Number of years the system is expected to be in service. An AIS is considered obsolete when its life cycle exceeds eight years and is no longer in production.

Costs (\$) :

Initial - Cost associated with initial procurement of system, including CPU, monitor, keyboard, operating software, application software and special add-on internal and external hardware items (e.g., printers, CD ROM drive, tape backup, additional RAM).

Consumables - Cost of consumables throughout the life cycle of the system to maintain the IS operational. This includes printer ribbons, laser printer toner and cleaning materials. This also includes printer paper or floppy disks.

Repair - Cost of repairs throughout the life cycle of the system. This includes cost of replacing portions of the system in lieu of repair. This does not include preventative maintenance costs.

Upgrades -

Hardware (Internal) . Cost of upgrading hardware items internal to the CPU box throughout the life cycle of the system. These costs are incurred following the initial purchase due to the technological advances and expanded functions of the system.

Hardware (External) . Cost of upgrading hardware items external to the CPU box throughout the life cycle of the system. These costs are incurred following the initial purchase due to technological advances and expanded functions of the system.

Software. Cost of new software or changes in existing software versions throughout the life cycle of the system. These costs are incurred following the initial purchase due to technological advances, expanded functions of the system and revisions to software.

TOTAL - Initial costs of the system added with the costs of consumables, repair and upgrades throughout the life cycle of the system.

30 Jul 98

INSTRUCTIONS

Each DEPARTMENT specify themselves by code number. Use each sheet for only one quarter (QTR) of a fiscal year (FY) . Mark Page number of total number of pages for the FY.

System: Specify number assigned to the IS by the AIS Security Officer and used in configuration control. If specifying a new system with no assigned number, write in a sequential letter (I.e., A, B, C...) .

Term: Specify terminal number assigned to the AIS by the AIS Security Officer and used in configuration control. If specifying a new terminal with no assigned number, write in a sequential letter (i.e., A, B, C...) . If the AIS not part of the network, leave blank.

INT: Check if hardware item is internal to the CPU box.

EXT: Check if hardware item is external to the CPU box.

Nomenclature: Specify the hardware item generic name and technical specifications that must be satisfied (e.g., Laser Printer - 8 ppm, black and white, front to back) .

Justification: Specify why hardware item is required for the system. Should include short description of hardware items= use in the system. Reference applicable System Decision Paper (SDP) or Abbreviated System Decision Paper (ASDP)by designation.

BACK OF ENCLOSURE(6)

INSTRUCTIONS

Each DEPARTMENT specify themselves by code number.
Use each sheet for only one quarter (QTR) of a fiscal year (FY) .
Mark Page number of total number of pages for the FY.

System: Specify number assigned to the IS by the AIS Security Officer and used in configuration control. If specifying a new system with no assigned number, write in a sequential letter (i.e., A, B, C...) .

Term: Specify terminal number assigned to the AIS by the AIS Security Officer and used in configuration control. If specifying a new terminal with no assigned number, write in a sequential letter (i.e., A, B, C...) . If the AIS not part of a network, leave blank.

Nomenclature: Specify the software item manufacturer, title names and version (e.g., **Fifth Generation Direct Access** version 5.0) .

Media: Specify media size and type (e.g., HD 3.5 or DD 5.25) .

Justification: Specify why software item is required for the system. Should include short description of software item=s application in the system. Reference applicable System Decision Paper (SDP) or Abbreviated System Decision Paper (ASDP) by designation.

AIS REPAIR REQUEST

Date: _____

MEMORANDUM

From: AIS System Security Officer, System _____
To: AIS Security Officer

Via: AIS Department Security Officer, Code _____
Department Department Head, Code _____

Subj: AIS REPAIR REQUEST

1. Request evaluation for repairs to AIS:

System	Terminal	Nomenclature	Building	Room

2. Point of contact:

Rank and Rate	First and Last Name	Room Extension

3. Description of symptoms/malfunction:

4. Actions already taken/initiated:

**SAMPLE
MEMORANDUM**

Date: _____

From: AIS Security Officer
To: AIS Department Security Officer, Code _____

Subj: AIS REPAIR REQUEST

Ref: (a) AIS Repair Request, System _____, dtd _____

1. Evaluation results for reference (a) follow:

2. Take the following action:

3. Procurement of repair/replacement items does not require an Acquisition Strategy Plan. However, requisition documentation must be submitted to the AIS Security Officer for review within thirty (30) days of this memorandum.

INFOSEC INCIDENT REPORT

Date: _____

From: AIS System Security Officer, System _____
To: AIS Security Officer

Via: (1) AIS Department Security Officer, Code _____
(2) Department Head, Code _____

Subj: INFORMATION SYSTEMS SECURITY INCIDENT

Ref: (a) NAVSUBSCOLINST 5239.2C

Encl: (1) INFOSEC Incident Summary

1. An INFOSEC Incident is reported in accordance with reference (a):

a. System Number: _____

b. Incident Date: _____ Time: _____

c. Nature of incident (check all that apply) :

	Accidental		Intentional
	Unauthorized Access		Malicious Code
	Unauthorized Disclosure		Unauthorized Modification
	Unauthorized Destruction		Denial of Service
	Other:		

2. Enclosure (1) is a brief description of the incident.

INFOSEC VIOLATION REPORT

Date: _____

From: AIS Security Officer
To: Commanding Officer

Via: (1) Information Systems Security Manager
(2) Executive Officer

Subj: INFORMATION SYSTEMS SECURITY VIOLATION

Ref: (a) NAVSUBSCOLINST 5239.2C

Encl: (1) INFOSEC Violation Summary

1. An INFOSEC Violation is reported in accordance with reference (a):

a. System Number: _____

b. Violation - Date: _____ Time: _____

c. Nature of Violation (check all that apply):

<input type="checkbox"/>	Unauthorized Disclosure
<input type="checkbox"/>	Unauthorized Modification
<input type="checkbox"/>	Unauthorized Destruction
<input type="checkbox"/>	Denial of Service
<input type="checkbox"/>	Other:

2. Enclosure (1) is a brief description of the violation.

3. The following action has been taken in respect to Information Systems Security (check all that apply) :

<input type="checkbox"/>	Operation continued with Accreditation
<input type="checkbox"/>	Accreditation; System on Accreditation Schedule
<input type="checkbox"/>	Operation continued with Interim Authority to Operate
<input type="checkbox"/>	Operation Restricted Pending Interim Authority to Operate

INFOSEC NON-DISCLOSURE AGREEMENT

Information System (IS) End User:

Last Name	First Name	MI	Rank/Rate
Department	Code	Phone Extension	PRD/Loss Date

ADP System Security Officer:

DAA: () CO, NAVSUBSCOL () Other:

Last Name	First Name	MI	Rank/Rate
Department	Code	Phone Extension	PRD/Loss Date

1. Agreement. I have been indoctrinated in the Information Systems Security (INFOSEC) Program by an ADP System security Officer and agree to the following provisions:

a. To read and comply with the INFOSEC Program instruction (NAVSUBSCOL 5239.2 series), Security Operating Procedures (NAVSUBSCOL 5239.2 series) and special procedures before operating any information system at Naval Submarine School.

b. To not disclose data acquired, transmitted, processed, displayed or stored on any Department of Defense or contractor information system to personnel without appropriate clearance and need-to-know. This includes all levels of classification. At no time will I discuss any data used at Naval Submarine School with the public.

c. To not disclose the capabilities, functions or uses of information systems operated or stored within Naval Submarine School spaces to the public or those without need-to-know.

d. Personnel utilizing the LAN shall observe the following prohibitions, restrictions and limitations.

(1) CLASSIFIED INFORMATION SHALL NOT BE SENT, RECEIVED, ACCESSED, STORED, DISTRIBUTED, TRANSMITTED, VIEWED, DISPLAYED, OR PROCESSED IN VIOLATION OF ESTABLISHED POLICIES PERTAINING TO THE HANDLING OF CLASSIFIED MATERIAL.

(2) PROPRIETARY, SENSITIVE, OFFICIAL USE ONLY, AND PRIVACY ACT PROTECTED INFORMATION SHALL NOT BE SENT, RECEIVED, ACCESSED, STORED, DISTRIBUTED, TRANSMITTED, VIEWED, DISPLAYED, OR PROCESSED IN VIOLATION OF ESTABLISHED POLICIES PERTAINING THERETO.

(3) SOFTWARE AND RELATED MATERIALS SHALL NOT BE OBTAINED, INSTALLED, COPIED, PASTED, TRANSFERRED OR USED IN VIOLATION OF PATENT, COPYRIGHT, TRADE SECRET OR LICENSING LAWS AND AGREEMENTS.

Enclosure (11)

(4) MALICIOUS SOFTWARE CODES, INCLUDING WITHOUT LIMITATION VIRUSES, LOGIC BOMBS, WORMS AND MACRO VIRUSES, SHALL NOT BE KNOWINGLY WRITTEN, CODED, COMPILED, STORED, TRANSMITTED OR TRANSFERRED.

(5) CHAIN LETTERS OR CHAIN JOKES SHALL NOT BE WRITTEN, FORWARDED OR PROCESSED IN ANY MANNER.

(6) RELIGIOUS MATERIALS SHALL NOT BE DISSEMINATED OUTSIDE ESTABLISHED COMMAND RELIGIOUS PROGRAMS.

(7) PARTISAN POLITICAL ACTIVITIES SHALL NOT BE PROMOTED OR ENGAGED IN, IN VIOLATION OF ESTABLISHED POLICY.

(8) FUND-RAISING ACTIVITIES SHALL NOT BE ENGAGED IN, UNLESS THE ACTIVITY IS SPECIFICALLY APPROVED BY THE COMMAND.

(9) PERSONAL FINANCIAL ACTIVITIES AND COMMERCIAL SOLICITATION; GAMBLING, WAGERING AND PLACING BETS; AND, POSTING PERSONAL HOME PAGES IS PROHIBITED, AS IS PERSONAL ENCRYPTION OF ELECTRONIC COMMUNICATIONS.

(10) RACIST, HATE-RELATED OR SUPREMACIST INFORMATION SHALL NOT BE SENT, RECEIVED, ACCESSED, STORED, DISTRIBUTED, TRANSMITTED, VIEWED, DISPLAYED, OR PROCESSED IN ANY MANNER.

(11) PORNOGRAPHY AND ANY OTHER MATTER OF A SEXUAL NATURE WHICH, IF VIEWED BY ANOTHER, WOULD CREATE A HOSTILE WORK ENVIRONMENT IN VIOLATION OF NAVY SEXUAL HARASSMENT POLICIES SHALL NOT BE SENT, RECEIVED, ACCESSED, STORED, DISTRIBUTED, TRANSMITTED, VIEWED, DISPLAYED OR PROCESSED IN ANY MANNER.

(12) PERSONAL USE OF THE INTERNET MUST BE REASONABLE IN FREQUENCY AND DURATION WITH NO ADVERSE IMPACT ON READINESS, MISSION ACCOMPLISHMENT, OR PERFORMANCE OF OFFICIAL DUTIES.

e. I also understand that ***the prohibitions, restrictions, and limitations imposed are punitive***, and that violations may result in adverse administrative or disciplinary action.

2. Signatures:

_____ IS End User

_____ Date

_____ Witness

_____ Date

ADP System Security Officer

NAVSUBSCOLINST 5239.2C CH-1
01E
26 May 1999

NAVSUBSCOL INSTRUCTION 5239.2C CHANGE TRANSMITTAL ONE

Subj: INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM

Encl: (1) INFOSEC Non-Disclosure Agreement

1. Purpose. To promulgate changes to basic instruction.

2. Action. Make the following changes:

a. Page 1, add enclosure (11), "INFOSEC Non-Disclosure Agreement", beneath enclosure (10).

b. Insert enclosure (11) after enclosure (10) in the basic instruction.

c. Page 12, paragraph j (2), insert "enclosure (11)" after the word "statement,".

d. Annotate the cover page, upper right hand corner "CH-1 entered (date) by (initials)".

J. J. GORDON
By direction

Distribution
CD ROM