



DEPARTMENT OF THE NAVY
CHIEF OF NAVAL EDUCATION AND TRAINING
250 DALLAS ST
PENSACOLA FLORIDA 32508-5220

CNETINST 5239.1B

IM1

(R)

27 MAY 1998

CNET INSTRUCTION 5239.1B

Subj: SECURITY REQUIREMENTS AND RESPONSIBILITIES FOR AUTOMATED INFORMATION SYSTEMS (AISs)

Ref: (a) OPNAVINST 5239.1A
(b) Public Law 100-235 Jan 8, 1988 (Computer Security Act of 1987)
(c) DoD Directive 5200.28
(d) SECNAVINST 5239.3 (R)
(e) SECNAVINST 5000.2B (R)
(f) OPNAVINST C5510.93E
(g) OPNAVINST 5510.1H
(h) NAVSOP 5239-29
(i) NAVSOP 5239-04 (R)
(j) NAVSOP 5239-26
(k) NAVSOP 5239-07 (R)
(l) NAVSOP 5239-08 (A)

1. Purpose

a. To ensure compliance with Department of the Navy (DON) AIS security requirements.

b. To identify Naval Education and Training Command (NAVEDTRACOM) activities' AIS security responsibilities.

c. To inform activities of changes affecting AIS security requirements and related responsibilities.

d. To highlight and provide guidance in specific areas which may cause accreditation delays.

2. Cancellation. CNETINST 5239.1A

3. Scope. This instruction applies to all organizational components of the Chief of Naval Education and Training (CNET) claimancy and addresses all elements of AIS security. All AISs being developed, maintained, managed, operated, or used by NAVEDTRACOM activities are covered by this instruction.

4. Objective. To provide centralized guidance and uniform policy on all aspects of AIS security. The objective for each NAVEDTRACOM activity is to establish and maintain an effective Risk Management Program and achieve accreditation for all AISs, networks, and computer resources based on the results of the security accreditation process.

27 MAY 1998

5. Background. References (a), (b), (c), and (d) establish requirements for the DON AIS Security Program. This instruction addresses activity responsibility for compliance with AIS security directives.
6. Definitions. Definitions applicable to this instruction are contained in reference (d).
7. Policy. All activities having computer resources or designing computer applications will establish and maintain an AIS Security Program in accordance with this instruction and references (a) through (l), as applicable.
8. Responsibilities. Designated Approving Authority (DAA) is the commanding officer unless otherwise directed. The DAA is responsible for formally granting accreditation for up to three years or Interim Authority To Operate (IATO) for up to one year in accordance with references (a) and (d). All AIS(s) under operational control of the activity must be accredited or be addressed by IATO based upon an acceptable level of risk. DAAs shall:
- a. Protect all AIS(s), networks, and computer resources against accidental or intentional destruction, unauthorized disclosure, denial of service, and unauthorized modification to ensure the availability of reliable information and automated support required to meet the activity mission.
- R) b. Ensure an Information System Security Manager (ISSM) and accompanying security staff (i.e., Network Security Officer(s) (NSOs) and Information System Security Officer(s) (ISSOs)) are identified and informed of their responsibilities. The ISSM position requires formal training. Formal training is optional for NSOs and ISSOs. Naval INFOSEC distributes training advisories. References (a), (i), (k), and (l) address activity AIS security staff requirements and duties.
- c. Identify security deficiencies through the accreditation process and, if these deficiencies are serious enough to preclude accreditation, take appropriate corrective action to achieve an acceptable level of security by implementing and maintaining
- A) safeguards and countermeasures to acquire accreditation. Review applicable Navy Staff Officer Publication (NAVSO Pub) 5239 (see DON INFOSEC Web Site) for guidance.
- d. Ensure data ownership is established for each AIS, to include accountability, access rights, and special handling requirements.
 - e. Ensure all AIS networks or other computer resources follow the least privileged principle, providing users the most restrictive set of privileges needed for the performance of authorized tasks. Each user is granted access only to the

27 MAY 1998

information which the user is entitled by virtue of security clearance or formal access approval and only to the resources necessary to perform assigned functions. In the absence of a specific positive grant of access, user access defaults to no access. The application of this principle limits the damage that can result from accident, error, or unauthorized use. (D)

f. Consider security policies throughout the life cycle of an AIS from the beginning of concept development through design, development, operation, and maintenance until replacement or disposal. Refer to references (a), (c), (d), and (e) with associated implementing directives and guidelines.

g. Be responsible for determining contingency plan requirements for AISS under their purview.

h. Ensure compliance with reference (b) which states that mandatory periodic training in computer security awareness and accepted computer security practice must be provided to all employees who are involved with the management, use, or operation of an AIS.

9. Guidance

a. When processing classified information, activities must comply with all previously mentioned computer security instructions and references (f) and (g). Reference (f) addresses TEMPEST requirements. Reference (g) addresses Information and Personnel Security Program Regulations. Both references (f) and (g) fall under the purview of the Security Manager. A coordinated effort must exist between the Security Manager and ISSM when processing classified information. (R)

b. Proprietary software must be used in a manner consistent with the manufacturer's license agreement. Reference (h) is a guidebook that addresses controls over copyrighted computer software. A responsible officer should be identified by the commanding officer to ensure compliance with reference (h).

c. Reference (d) states that an accreditation of DON information systems shall be performed by competent management personnel in a position to balance operational mission requirements and the residual risk of system operation. All accreditation decisions shall be documented. (R)

d. To ensure compliance with AIS security policies throughout the life cycle of an AIS, network, or other computer resource, developing activities will ensure the early and continuous involvement of the users, security staff, data owners, and DAAs in defining and implementing the security requirements. Acquisition and procurement specifications must identify security requirements. To the maximum extent possible, computer security will be built into systems so users are relieved of the responsibility to develop security procedures and controls for their system(s). (D)

27 MAY 1998

e. Reference (j) addresses Remanence Security. Remanence refers to traces of information remaining on data storage media after the use of insufficient purging procedures. Remanence security provides methods and procedures to prevent disclosure of classified and/or unclassified but sensitive information to persons who do not have the proper clearance and need-to-know for that information.

f. All Navy AIS(s) are required to display a CNO legally approved LOG-IN warning banner. The banner should be displayed at the first point in the log-in process and include an option

- A) that allows halting of the log-in process by the user. The most current version of the LOG-IN warning banner can be downloaded
D) from the DON INFOSEC Web Site.

- A) g. The threat of attack from computer viruses and other malicious code is significant, and often the result of opening an e-mail attachment or downloading remote files. Successful prevention includes the use of anti-virus software and the establishment of command policy and procedures to minimize the introduction of malicious code. Department of Defense licensed anti-virus software is available free to all DON activities and may be downloaded from the DON INFOSEC Web Site.

- A) 10. DON INFOSEC Web Site. The DON INFOSEC Web Site on the World Wide Web provides access to the DON Information Assurance (IA) Publications, as well as other IA related references, advisories and announcements, Antivirus Tools, and a variety of resources on IA issues across DON, the Department of Defense, and other services and agencies. Access the Web Site on the Non-classified INTERNET Protocol Router Network (NIPRNET) at <http://infosec.navy.mil>, or on the Secret INTERNET Protocol Router Network (SIPRNET) at <http://infosec.navy.smil.mil>. Navy INFOSEC has a Naval Computer Incident Response Team (NAVCIRT) which can be reached at 1-800-628-8893, 1-888-NAV-CIRT 628-2478, DSN 537-4024, or commercial (757) 417-4024.

11. Action. NAVEDTRACOM activities will implement this instruction to ensure that an AIS security program is established and maintained.

- R) 12. Point of Contact. The CNET point of contact for AIS security is Naval Education and Training Professional Development and Technology Center (NETPDTC) (N644), DSN 922-1001 ext 1363 or commercial (850) 452-1001 ext 1363. NETPDTC (N644) manages the NAVEDTRACOM AIS security program.



R. M. SCOTT
Chief of Staff

27 MAY 1998

Distribution (CNETINST 5218.2B):
Lists I through IX
SNDL FT72 (DPTNAVSCI)
FT74 (NROTCU)

Stocked:
CHIEF OF NAVAL EDUCATION AND TRAINING
CODE 0041
CNET
250 DALLAS ST
PENSACOLA FL 32508-5220

