



DEPARTMENT OF THE NAVY
NAVAL EDUCATION AND TRAINING PROFESSIONAL
DEVELOPMENT AND TECHNOLOGY CENTER
6490 SAUFLEY FIELD ROAD
PENSACOLA, FLORIDA 32509-5237

NETPDTCINST 5239.1A
N6A

IN REPLY REFER TO:

05 JUN 2002

NETPDTC INSTRUCTION 5239.1A

Subj: **AUTOMATED INFORMATION SYSTEM (AIS) SECURITY**

Ref: (a) SECNAVINST 5239.3
(b) OPNAVINST 5239.1B
(c) CNETINST 5239.1B
(d) DOD INSTRUCTION 8510.1 (DITSCAP)

Encl: (1) Automated Information Systems (AIS) Security
Guidelines

1. **Purpose.** To implement references (a) through (d) and establish the Department of the Navy AIS Security Program for Naval Education and Training Professional Development and Technology Center (NETPDTC).
2. **Cancellation.** NETPDTCINST 5239.1
3. **Revision.** Since this is a major revision, marginal notations are not annotated. This revision should be read in its entirety.
4. **Scope.** This instruction applies to all organizational components of NETPDTC and addresses AIS security policy and responsibility for NETPDTC employees. Key elements required by reference (d) for all NETPDTC AIS Security Plans are included in this instruction. For specific information on the Privacy Act, ADP Contingency Planning, and Copyright Infringement, refer to appropriate directives.
5. **Objective.** To provide centralized guidance and uniform policy on all aspects of AIS security. The NETPDTC AIS Security Program will ensure that all AIS hardware, products, data files, software, and services are adequately protected against accidental or deliberate destruction, unauthorized modification, unauthorized disclosure, and denial of service.

05 JUN 2002

6. **Policy**. To ensure compliance with Department of Defense, Navy, and CNET AIS security directivities, all NETPDTC personnel will become familiar with this instruction to protect computers, networks, and data by the continuous employment of AIS security policy and protective features. Personnel assigned specific AIS security responsibilities will ensure compliance with this instruction. All employees will become familiar with enclosure (1).

7. **Responsibilities**

a. **Designated Approving Authority (DAA)**. The Commanding Officer is the DAA for NETPDTC AIS(s). The DAA is responsible for formally granting authority to operate AIS(s) based upon an acceptable level of risk. This risk level is addressed in the System Security Authorization Agreement (SSAA) directed by reference (d). The DAA for CNET Enterprise Network (CENet) and distributed CNET applications is CNET CIO, however, NETPDTC application system Project Managers must prepare and maintain their respective SSAA.

b. **Information System Security Manager (ISSM)**. The ISSM shall be formally designated, in writing, by the Commanding Officer. This position is located in the Systems Engineering and Technology Services Department, N6, and shall serve as the claimancy ISSM responsible for managing the CNET Headquarters AIS Security Program as prescribed in references (a), (b), (c) and (d). The claimancy ISSM is responsible for interpreting and tailoring DOD and DON security policy to meet the requirements of the command. Directors of NETPDTC remote sites shall be assigned ISSM responsibility by the claimancy ISSM, in writing, for their respective locations and will confer with the claimancy ISSM on AIS security issues. The claimancy ISSM shall also appoint an Assistant ISSM to manage NETPDTC's AIS Security Program and related local requirements. The claimancy ISSM shall ensure all ISSMs receive appropriate training in AIS security policy and practices.

c. **Information System Security Officer(s) (ISSO(s))**. ISSO responsibility is assigned to all NETPDTC Branch Heads. Appropriate managers of codes not subdivided to the branch level must assign an ISSO. The Branch Head may delegate ISSO responsibilities, in writing, to one or more personnel having a

05 JUN 2002

working knowledge of specific AIS(s). The function of the ISSO is to address Information Technology (IT) security for the protection of all AIS(s), networks, and computer resources within their area of responsibility to ensure the availability of reliable information and automated support required to meet the activity mission. ISSO responsibilities are as follows:

(1) Address security matters for the AIS(s) under your cognizance and ensure that personnel are aware of security responsibilities listed in enclosure (1). Consult with ISSM as needed.

(2) Execute the AIS Security Program as it applies to your area of responsibility, including the preparation and submission of accreditation support documentation. The accreditation process is used to identify and correct security deficiencies. Contact the ISSM when a significant change affecting the AIS security posture occurs.

(3) Ensure only authorized users with a need to know have access to IT resources.

(4) Serve as point of contact on network security issues in coordination with network administrators and AIS security staff.

(5) Implement security countermeasures/safeguards necessary to maintain a satisfactory level of operational security in a cost-effective manner as required by references (a), (b), (c), and (d) in coordination with ISSM.

(6) Ensure that AIS users in your area of responsibility are granted access only to the information and resources necessary to perform assigned functions. This access is to be removed when the employee no longer has a work related need for access.

(7) Ensure all Navy AIS(s) display the CNO legally approved LOG-IN Warning Banner. The banner should be displayed at the first point in the log-in process.

(8) Assist the ISSM in implementing a comprehensive AIS security program by ensuring compliance with this instruction.

05 JUN 2002

ISSOs can implement additional security requirements applicable to their area of responsibility.

(9) Report any actual or suspected IT security violation or incident to the ISSM. Contact the ISSM for assistance as needed.

d. Network Security Officer (NSO). The NSO is responsible for implementing and maintaining network security. The Director of the Systems Software and Hardware Engineering Division, N62, serves as the CNET Enterprise Network (CENet) NSO. For NETPDTC Local Area Networks (LANs), the branch head is the NSO unless otherwise delegated in writing. The NSO is responsible for the following:

(1) Ensuring that standard security procedures and measures that support the security of the entire network are developed and implemented.

(2) Ensuring the network is in compliance with Navy and DOD policies.

(3) Reporting the security status of the network to the ISSM, as needed.

(4) Ensuring the accountability and protection of network assets.

(5) Reporting network security incidents to the ISSM when the network is compromised.

(6) Initiating protective or corrective measures if a security problem is discovered.

(7) Performing risk management functions required for preparation and maintenance of the network SSAA.

(8) Consult with ISSM as needed.

e. Central Design Activity (CDA). Every Navy activity that designs, develops, converts, implements, modifies, or operates an AIS must provide for the implementation and maintenance of required AIS security safeguards. NETPDTC

05 JUN 2002

Application System Project Managers will consider security policies throughout the life cycle of an AIS from the beginning of concept development through design, development, operations and maintenance until replacement or disposal. Application System Project Managers will ensure the early and continuous involvement of the users, security staff, data owners and Designated Approving Authority in defining and implementing 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).

All applications developed and/or maintained by NETPDTC must be in accordance with reference (d). A primary requirement of reference (d) is the System Security Authorization Agreement (SSAA). The SSAA documents decisions, specifies IA requirements, documents the required level of Certification and Accreditation (C&A), documents operational system security and identifies possible solutions to IT security issues. An SSAA shall be developed by the Application System Project Manager for each system being accredited. The SSAA will be certified by both the Application System Project Manager and ISSM. It will then be sent to the Designated Approving Authority (DAA) who will sign the Accreditation Statement based on the SSAA support documentation and certification statement. The SSAA must be reviewed and the application reaccredited every three years or sooner if significant changes occur.

f. Transmission Of Sensitive But Unclassified (SBU) Information. Public Key Infrastructure (PKI) and Virtual Private Network (VPN) policy for transmission of SBU including Privacy Act information: there are two acceptable methods using data encryption; by the use of DOD PKI or via PKI enabled VPN.

g. WEB Servers. In order for NETPDTC to maintain trusted network status, WEB servers must conform to Secure Socket Layer (SSL)/PKI infrastructure.

h. Information Assurance Vulnerability Alert (IAVA). The Navy has established the IAVA process to provide positive

05 JUN 2002

control of the vulnerability notification and corrective action process. The claimancy ISSM and respective remote site ISSMs will coordinate the required action with the organizational units affected by the specific IAVA vulnerability identified. Corrective action must be taken within the timeframe established by CNET CIO.

i. Information Operations Condition (INFOCON) Compliance. INFOCON is a comprehensive Computer Network Defense (CDN) consisting of different levels to uniformly heighten or reduce Computer Network Defense posture to defend against adversarial attacks on computers and networks. System operability could be impacted under a heightened INFOCON level. Employees involved will be notified to take required action in accordance with the specific attack and current INFOCON level.

8. Action

a. Department Heads, Unit Directors, Division Directors, Special Assistants, and appropriate NETPDTC managers will ensure their employees are made aware of the responsibilities identified in this instruction.

b. The Claimancy ISSM is the focal point for CNET AIS security matters and should be contacted whenever AIS security assistance is needed.

9. Point of Contact. Claimancy ISSM, N6A, telephone 452-1001, extension 1363 or 1134.



G. B. DYE

Distribution: (NETPDTCINST 5216.1E)
Lists I, IA, and II

Web Access: MAIN INDEX
<https://pennd09.cnet.navy.mil/netpdtc/directives.nsf>

05 JUN 2002

AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY GUIDELINES

1. Government computers are to be used for official projects only. Examples of prohibited use include, but are not limited to the following:

a. Illegal, fraudulent or malicious activities.

b. Activities whose proposes are for personal or commercial financial gain. These activities include solicitation of business services or sale of personal property.

c. Unauthorized fundraising.

d. Accessing, storing, processing, displaying or distributing offensive or obscene material such as pornography or hate literature.

e. Obtaining, installing or using software obtained in violation of the appropriate vendors patent, copyright, trade secret or license agreement.

f. The creation, forwarding, or passing of chain letters.

2. No classified information can be processed on a Work Station until authorized by the ISSO, ISSM and the Security Manager. No classified information is authorized on any Work Station connected to the CNET Enterprise Network (CENet)

3. DON unclassified AISs are considered sensitive. This means that all Work Stations processing unclassified information must, at a minimum, safeguard that information and equipment against tampering and destruction.

4. Passwords are one of the simplest, most effective security measures, but are often the first target of intruders. Passwords shall be managed in accordance with the below guidelines and tailored to the appropriate level of protection required.

a. Passwords shall be a minimum of eight characters in length, consisting of a mixture of alphanumeric characters

Enclosure (1)

05 JUN 2002

(i.e., a-z, A-Z and 0-9). Easily guessed passwords should be avoided as well as words found in any dictionary. Names of family members, pets, social security numbers, addresses, telephone numbers and dates of personal importance should not be used.

b. Default passwords at the system or network administrator level shall be changed to a unique password upon system installation.

c. Passwords shall be changed semi-annually (180 days) at a minimum.

d. Reuse of a previously employed password is prohibited.

e. User identifications and passwords will not be posted in the work area.

f. User access (password) must be removed when the user leaves the command or is assigned duties that no longer require access.

5. Computer printed reports should be properly labeled for distribution. When reports contain classified data, contact the Security Manager for proper marking and handling procedures. When reports contain sensitive unclassified data requiring special protection such as Privacy Act Data, each report must be labeled (example: "Privacy Act Sensitive", "Privacy Act Protected", or "Privacy Act Sensitive, disclose on a need to know basis only").

6. Removable storage media containing Sensitive But Unclassified (SBU) or Privacy Act Information will be externally labeled. Handling procedures need to be established for sensitive unclassified information (reports and removable storage media) to reasonably protect data based on employee need to know. In a mixed (same work area) classified and unclassified environment, all removable storage media must be labeled.

7. Users have a responsibility to protect their computer monitor from being viewed by others that do not have a work

05 JUN 2002

related need to know when classified or sensitive unclassified data is accessed on the monitor. For unclassified systems a screen saver password routine can be used when the workstation is unattended.

8. For virus protection users should have current antivirus software loaded on all Work Stations. For assistance contact NETPDTC Customer Assistance. Many NETPDTC users are on managed update that automatically installs the current antivirus signature. The antivirus software can only protect you from known viruses and other types of malicious code. Many new viruses use Microsoft Outlook Mail to spread rapidly. If you open an attachment from your Inbox but your mouse pointer stays in the shape of an hour glass and your Outbox count is rising (indicating mail you are sending) you likely have become infected and spreading the virus. If this happens, immediately power your system off and contact customer assistance. Be cautious and never open a suspicious attachment even if it is from someone you know.

9. Virus hoaxes contain bogus warnings and usually arrive in the form of an email. The best course of action is to delete these hoax e-mails. The DOD Antivirus Team sends out notification of serious virus threats. Distribution of DOD notification will be made accordingly. Information on virus hoaxes can be found at <http://www.europe.datafellows.com/news/hoax>. This source is recommended by NAVY INFOSEC.

10. Report all AIS security incidents to your ISSO (Branch Head).