



DEPARTMENT OF THE NAVY
NAVAL DENTAL CENTER SOUTHWEST
2310 CRAVEN ST.
SAN DIEGO, CALIFORNIA 92136-5596

NDCSWINST 5239.1D
02MID
27 April 1999

NAVDENCEN SOUTHWEST INSTRUCTION 5239.1D

Subj: AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM (AISSP)

Ref: (a) SECNAVINST 5239.3
(b) SECNAVINST 5211.5D
(c) NAVDENCENS DIEGOINST 5230.1D
(d) NAVSUPINST 4200.85C

Encl: (1) AISSP for Naval Dental Center Southwest (NDCSW)
(2) Contingency Plan

1. Purpose. To promulgate NDCSW's Automated Information System (AIS) Security Program and assign responsibilities within guidelines of references (a) through (d). This instruction establishes a comprehensive new plan for AIS security, appropriate use, and risk assessment and should be read in its entirety.

2. Cancellation. NAVDENCENS DIEGOINST 5239.1C and NAVDENCENS DIEGOINST 5239.2B.

3. Definitions

a. Office Information System (OIS): Type of Automatic Data Processing Office (ADPO) equipment primarily limited to document text preparation.

b. Data: Includes all information processed, handled, or otherwise manipulated by an Automatic Data Processing (ADP) system, OIS or network.

c. Hardware: The physical components of a system, e.g., keyboards, disk drives, computers, and printers.

d. Software: Programs, procedures and documentation associated with a computer system

e. Media: Memory storage for software, e.g. tape, floppy disk, hard disk.

f. Hard Copy: A copy of data reduced to paper.

g. Abbreviated Systems Decision Paper (ASDP). Documentation used to justify procurement of microcomputer systems.

NDCSWINST 5239.1D
27 April 1999

4. Background. References (a) and (b) established minimum AIS security structure, responsibilities and standards. In addition, it prescribes the Department of the Navy (DON) policy and procedures for implementing the Privacy Act of 1974 (Public Law 93-579) with regard to all personal data systems within the Department of the Navy.
5. Discussion. In compliance with the above references, risk assessment and contingency planning for command AIS are to be initiated and accredited when an adequate level of security has been attained. Achievement and maintenance of accreditation for all AIS systems within the command is mandatory.
6. Action. Enclosure (1) delineates and assigns responsibilities for implementation and review of compliance with Department of the Navy and Bureau of Medicine and Surgery policies on AIS Security at NDCSW. Enclosure (2) provides essential guidance for contingency preparation, emergency reaction, backup and restoration following occurrence of a contingency situation.


D. D. WOOFTER

Distribution:
List I, Case 1, 2

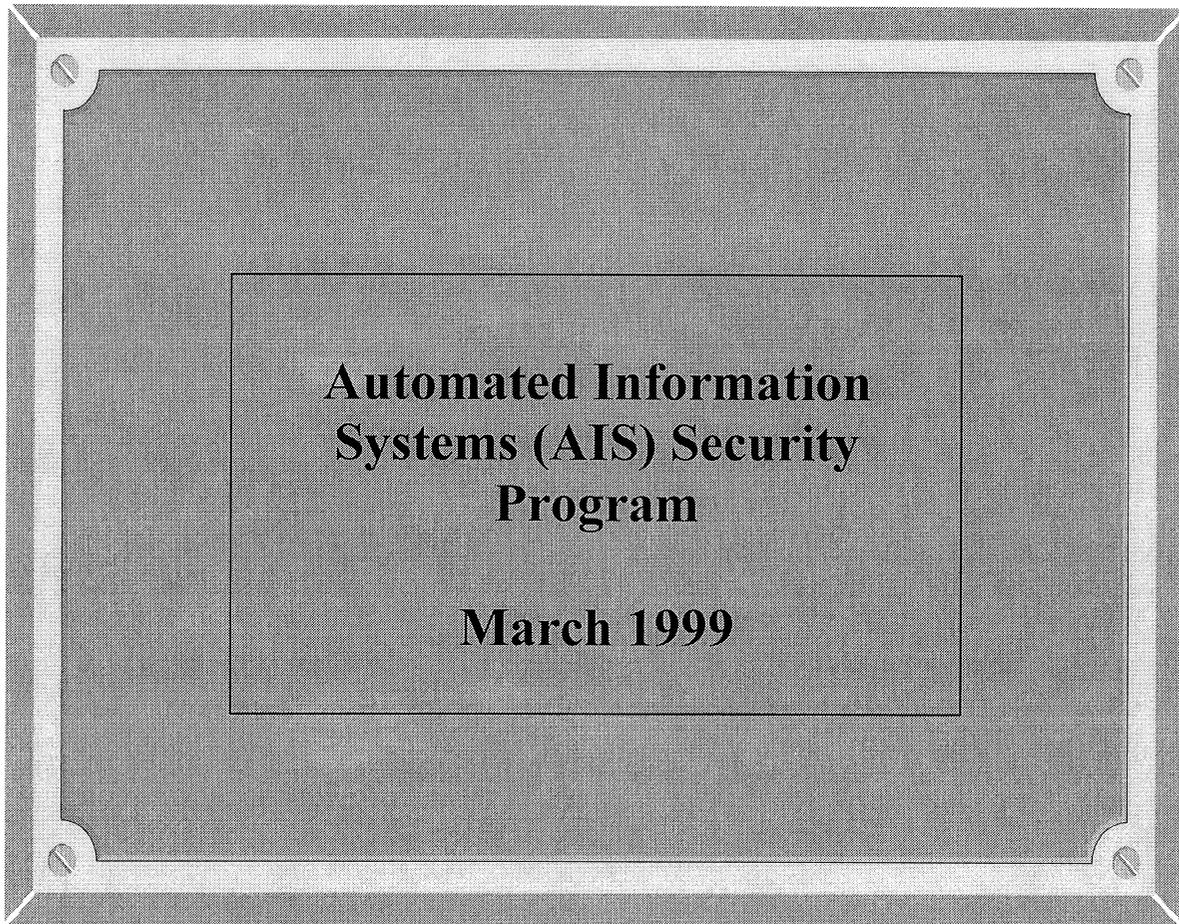


TABLE OF CONTENTS

Paragraph		Page
1.	Introduction	3
2.	References	3
3.	Scope	3
4.	Commanding Officer's Policy Statement	4
5.	Organization	5
6.	Specific Responsibilities	5
	Commanding Officer (CO)	5
	Security Manager (SM)	6
	Information Systems Security Officer (ISSO)	6
	ADP System Security Officer (ADPSSO)	7
	Network Security Officer (NSO)	8
	Terminal Area Security Officer (TASO)	8
	Physical Security Officer (PSO)	9
7.	AIS Security Objectives	9
8.	Current AIS Security Environment	10
9.	AIS Security Training	10
10.	Internal Control	11
11.	Life Cycle Management (LCM)	11
12.	Security In Software and Hardware Configuration Control	12
13.	Activity Accreditation Schedule (AAS)	12
APPENDIX A AIS SECURITY ORGANIZATION LINE DIAGRAM		13
APPENDIX B LISTING OF HARDWARE AND SOFTWARE		14
APPENDIX C ACTIVITY ACCREDITATION SCHEDULES (AAS)		15

NDC Southwest
ACTIVITY AUTOMATED INFORMATION SYSTEMS SECURITY PLAN (AAISSP)

1. Introduction. Per NDCSWINST 5239.1D, this plan is designed to provide information and guidance to all NDCSW personnel on measures to protect Command Automated Information Security (AIS) equipment, software, and data stored therein and provide contingency operating procedures in the event of loss of equipment, software, or data due to accidental or intentional acts.

2. References:

- (a) SECNAVINST 5239.3
- (b) SECNAVINST 5211.5D
- (c) NAVDENCENSIEGOINST 5230.1D
- (d) NAVSUPINST 4200.85C
- (e) Appendix A Diagram of the NDCSW AIS Security Organization
- (f) Appendix B Inventory of all AIS Hardware and Software
- (g) Appendix C NDCSW Activity Accreditation Schedule
- (h) SECNAVINST 7510.7C

3. Scope.

a. The Activity AIS Security Plan (AAISSP) for NDCSW serves as a central planning and managing tool in controlling the total security environment of all Automated Information Systems (AIS) under the command's cognizance. It documents the current AIS security environment, establishes individual accountability and security program objectives, and outlines a Plan of Action and Milestones (POA&M) to achieve and maintain AIS security accreditation.

b. The AIS Security Program, as implemented for NDCSW, provides for the active participation by all members and employees in the continual security of this command and the equipment and other resources identified herein. In addition to those regulations and instructions promulgated by Department of Defense, Department of the Navy, and Bureau of Medicine and Surgery, all security instructions issued by NDCSW also apply.

c. The NDCSW AIS Security Program applies to all AISs and networks which are either operated directly by NDCSW or operated on its behalf, as well as any other personnel who are authorized access to command AISs or data. Implementation of the command AIS Security Program requires active participation by all personnel in the continual security maintenance of command AIS resources, including computers, software and data. In addition to those regulations and instructions promulgated by DOD, DON, and BUMED; all physical, personnel and information security regulations issued by the Commanding Officer, NDCSW apply.

d. As changes occur in the NDCSW AIS environment, this AAISSP will be modified to incorporate those changes.

27 April 1999

4. **Policy Statement.**

a. NDCSW staff personnel, both military and civilian, are directed to comply with the guidelines established in this AAISSP.

b. AIS equipment at NDCSW includes AIS and telecommunications systems. These require protection against both accidental and deliberate disclosure of data or software to unauthorized personnel and against unauthorized modification, destruction or denial of services. It is the responsibility of each staff member to adhere to the requirements of the AAISSP and to report violations to the Information Systems Security Officer (ISSO). The requirements and limitations established by this AAISSP also apply to contractor-provided AIS support and to contracts operating AISs or networks for or on behalf of NDCSW. Any host-user agreements required under this activity will be in writing and concluded at the Commander, Commanding Officer level. Failure to comply with AIS security requirements will be cause for termination of any such arrangements.

c. Permission to operate personally owned hardware/software will be granted only by special waiver requiring approval of the Commanding officer per ref (c).

d. All actions processed by any NDCSW ADP device must be in keeping with Navy Core Values. At no time shall any item containing objectionable materials be accessed, entered, started or processed on any computing devices at NDCSW. E-mail and/or web browsing of a sexual, pornographic, explicit, or suggestive nature is expressly prohibited. In addition, racial ethnic or religious jokes, slurs or negative comments are prohibited. This paragraph constitutes a written order, the violation of which will subject involved personnel to disciplinary action.

e. Personal use of the internet and email functions are not in themselves prohibited. Proper decorum and common sense must be used when involved with these devices. Answering e-mail or searching the web involving government time will be kept to a minimum and not effect normal daily operational requirements. Accessing housing information for a PCS move or connecting with your sponsor are appropriate and encouraged use of these systems.

f. Personnel Security. All personnel (military, civil service, and contractors) employed by NDCSW will have security clearances appropriate to the highest level of data handled.

g. Administrative/Operating Procedures. Standard operating procedures (SOPs) and administrative directives shall be developed to ensure control of data/files utilized on personal computers (i.e. security level, privacy act infringements, integrity and efficiency aspects, and unauthorized use of DOD resources).

h. The security mode of AIS operations at NDCSW is "limited access" with the Designated Approving Authority (DAA) being the Commanding Officer. Level I (classified) data will not be processed on AIS equipment. Levels II & III data **only** will be processed on AIS equipment by NDCSW. Included are, privacy act data (Level II), for Official Use Only (Level II), administrative sensitive (Level II), fiscal restricted (Level II), and all others (Level III).

i. Due to the difficulty inherent in identifying and segregating NDCSW AIS equipment, all AIS systems will be accredited under the same procedures in accordance with ref (a).

j. Non-commercial software systems received as part of multiple activity distribution will be certified by the activity. Specifically, the ISSO will certify to the ADPSSO that the system was properly installed and that the system properly implements the appropriate function.

k. Random checks on command computers for appropriate use or abuse will be conducted by the Management Information Department on a monthly basis. Monthly reports will be retained by Management Information Department and any discrepancies shall be noted and forwarded to the Commanding Officer.

5. **Organization.**

a. AIS support is critical to the performance of the command's mission. Provision of this support is assigned to the Head, Management Information Department (MID). AIS security is included in this responsibility.

b. In accordance with references (a) and (b), an AIS Security Program is established for NDCSW. The AIS Security Officer (Head, Management Information Department) is appointed to implement the command's AIS Security Program and to ensure adequate security is maintained for all AISs within NDCSW cognizance.

c. ADPSSO and TASO will be assigned in writing by branch directors to assist in AIS security matters.

6. **Specific Responsibilities.**

a. **Commanding Officer.** The Commanding Officer, NDCSW is responsible for all activities and functions of the command. With specific regard to AIS security and the DON AIS Security Program, the Commanding Officer is responsible for compliance with Chapter 2 of reference (a). More specifically, the Commanding Officer must:

- (1) Establish AIS operational value and importance.
- (2) Specify operational controls.
- (3) Classify the asset and specify asset protection controls using a selective protection of assets approach.
- (4) Authorize access and assign custody of equipment and data to appropriate personnel.
- (5) Communicate control and protection requirements to custodians and users.
- (6) Monitor compliance and periodically review control and classification decisions.

27 April 1999

The Commanding Officer delegates monitoring responsibilities to the AIS Security staff. Such delegation does not dilute custodian, user, or program manager responsibility for compliance with AIS asset protection requirements. The command will take reasonable steps to understand conditions surrounding the custody, use, or development of assets, initiate appropriate actions when problems are identified, and participate in custodian, user, and developer risk assessment decisions.

b. **Security Manager.** The NDCSW Security Managers (SMs) are the principal advisors on physical and information security in the command. These are the key positions in the development of the Command's Information Security Program (ISP). Director for Dental Center Administration (DDCA) is the command security manager. The Head of Operating Management is responsible for physical security, and the Head, Management Information Department is responsible for information security. The security managers' responsibilities include but are not limited to the following:

- (1) Serve as the Commanding Officer's advisor and representative on matters of physical security of AIS equipment, security of data and information systems and security of classified information.
- (2) Develop Command Information Security Procedures.
- (3) Ensure compliance with accounting and control requirements for classified material.
- (4) Process personnel security clearance actions.
- (5) Administer the command's classification management requirements.
- (6) Coordinate the preparation of classification guidelines. (Level I, II, and III)
- (7) Ensure compliance with provisions of the industrial security program (OPNAVINST 5540.8K).
- (8) Formulate and coordinate security control and storage measures of classified material.
- (9) Establish security control of visitors.
- (10) Formulate and coordinate the physical and information security education program.

c. **NDCSW Information Systems Security Officer (ISSO).** The Commanding Officer will appoint, in writing, an Information Systems Security Officer (ISSO) for the command, along with an Assistant ISSO (AISSO) to act as a knowledgeable backup person. The ISSO and AISSO must be aware of the accreditation status of the command, the points of contact for the various ADP systems, and the current overall command ADP security posture. Letters of appointment will be reissued to reflect changes in the ADP security staff as they occur.

- (1) Coordinate with and assist the NDCSW security managers on matters concerning AIS security.
- (2) Develop, implement and maintain the AAISSP and milestones.
- (3) Develop and implement the Risk Assessment, Security Test and Evaluation, and Contingency Planning processes.
- (4) Ensure that all AIS security incidents or violations are investigated, documented and reported.
- (5) Prepare the AIS security accreditation support documentation.
- (6) Ensure that all AIS Security personnel are appointed in writing.
- (7) Assist ADPSSO in reviewing his/her plans procedures for completeness and adherence to policy.
- (8) Develop AIS security policies and standards consistent with reference (a).
- (9) Coordinate with the Information System Executive Board on matters concerning AIS security.

d. **ADP System Security Officers (ADPSSO).** An ADPSSO will be appointed for each NDCSW branch clinic having AISs by their respective branch directors and will:

- (1) Be the focal point for all security matters for the AIS(s) assigned.
- (2) Execute the AIS Security Program as it applies to the assigned AIS(s) including preparing and submitting accreditation support documentation.
- (3) Maintain an inventory of all AIS hardware, implemented system software releases, and major functional application systems (e.g., finance, personnel, logistics, etc.).
- (4) Monitor system activity. Identify levels and types of data handled by the AIS(s), verify assignment of passwords and review of audit trails, outputs, etc., to ensure compliance with security directives and procedures.
- (5) Conduct and document a risk assessment in accordance with reference (a). The risk assessment methodology to be used will be selected with concurrence of the DAA.
- (6) Assist the ISSO in the development and implementation of a comprehensive AIS activity and network security posture.

27 April 1999

(7) Supervise, test, and monitor, as appropriate, changes in the AIS system(s) affecting the AIS activity and network security posture.

(8) Implement appropriate countermeasures required by directive or determined to be cost-effective.

(9) Develop and test annually, all contingency plans as specified in reference (a).

(10) Monitor AIS procurement for security impact to ensure compliance with security regulations and known security requirements for the assigned AIS systems. Security regulations and requirements are established in accordance with ref (a).

(11) Ensure that all AIS security violations are reported to the ISSO.

(12) Manage the implementation and execution of the AIS Security Program as it applies to the particular AIS System.

(13) Ensure all AIS users are trained in AIS security.

e. Network Security Officers. The NDCSW Network Security Officer (NSO) will be appointed for the AIS network and will act as the Commanding Officer's staff advisor and the focal point for NDCSW AIS network security matters with the following major responsibilities:

(1) Ensure that countermeasures and requirements are included in the network design and that individual nodes of the network comply with these countermeasures and requirements, prior to interfacing with the network. The security requirements will be agreed to in writing by the network DAA and the AIS activity connected to the network. Networks having multiple service/agency members will be accredited jointly. Network accreditation will be based on the prior accreditation of each network node.

(2) Develop and promulgate the standard security procedures governing network operations.

(3) Ensure that security measures and procedures used at network modems fully support the security integrity of the network.

(4) Maintain liaison with ADPSSO.

(5) Ensure that all required countermeasures are utilized.

f. Terminal Area Security Officers (TASO). Terminal Area Security Officers will be appointed where applicable and will enforce all security requirements implemented by the ISSO/ADPSSO for remote terminal areas. Appointments will be made in writing by branch directors. TASOs will ensure that all countermeasures required to protect the remote areas are in place. The TASOs will be appointed according to the physical location of the terminals.

g. **The Physical Security Officer (PSO).** The Physical Security Officer is responsible for the overall physical security of NDCSW buildings. The entrance doors to the buildings housing the microcomputer systems are to be locked at the close of business. Additional physical security is provided at appropriate locations.

7. **AIS Security Objective.** The primary objectives of the NDCSW AIS Security Program are:

a. Accuracy. It is the intent of NDCSW to ensure that all data entrusted to AIS system storage and processing will be accurately maintained, i.e., it will remain as received from the owner of this information.

b. Availability. NDCSW will develop, maintain, and test contingency plans designed to prevent loss of data or minimize periods of non-accessibility to that data stored on AIS system(s).

c. Protection Against Disclosure. Security features available in the system software will be utilized at all times to prevent unauthorized disclosure of information.

d. Risk Management Program. NDCSW will maintain a risk management program to provide operational procedures designed to prevent disclosure or modification of information and lapses in AIS support.

e. Risk Assessment. NDCSW shall implement a security program based upon a risk assessment to determine how much protection is required and exists. The security program will be an ongoing effort that must be reevaluated whenever changes occur in the AIS environment.

f. NDCSW will consider these elements of AIS security in the security program.

- (1) physical.
- (2) personnel.
- (3) administrative/operating procedures.
- (4) communications.
- (5) hardware.
- (6) software.
- (7) data.

g. Accreditation. Six steps to achieving Command accreditation on each AIS system and network are itemized as follows:

- (1) Plan of Action and Milestones (POA&M)

- (2) Activity AIS Risk Assessment Team Charter
- (3) Risk Assessment
- (4) Contingency Plan
- (5) Security Test & Evaluation (ST&E)
- (6) Documentation and Request for Accreditation

8. Current AIS Security Environment.

- a. Access controls for all AISs are in place.
- b. Appendix B contains a descriptive list using location and bar code numbers of individual NDCSW AISs including hardware/software descriptions.
- c. Additional access controls are in place for individual office spaces based on the level of sensitivity.
- d. The NDCSW AIS Security Organization is listed in Appendix A.
- e. Due to continued addition or relocation of equipment, the NDCSW ISSO will coordinate new AIS Security Surveys as required.
- f. Police and fire protection are provided by the various bases which this command is a tenant.
- g. NDCSW is staffed by military, civil service, and contract personnel.
- h. Communication.
 - (1) Communication to/from NDCSW AIS is by local area networks and/or standard asynchronous modems and over commercial telephone lines.
 - (2) All users of NDCSW computer systems, including those seeking access from remote sites, are provided with security briefings before access is granted.
- i. Emanations. No top secret classified information is processed by AIS systems at NDCSW.

9. AIS Security Training.

- a. Training in AIS security will be the responsibility of the AIS Security Organization (Appendix A). Each member will receive formal and informal instruction on AIS Security. The

training program will follow requirements of Chapter 10 of reference (a). All personnel will receive a security brief and all employees will be required to be familiar with the NDCSW AIS Security Instructions. More specifically, the NDCSW AIS Security Training Plan will be:

- (1) Developed and maintained by the command ISSO.
- (2) Presented to all military, civilian, and contractor employees authorized access to

AIS assets:

- (a) Upon reporting aboard.
- (b) Annually thereafter.
- (c) Recorded in training records.
- (d) Conducted by AIS Security Staff and may be combined with command physical and information security training.

b. The subject matter of this training will include at a minimum:

- (1) Storage of AIS hardware and software.
- (2) Access authority to AIS equipment.
- (3) Password security.
- (4) Requirement and procedure for backup.
- (5) Security of equipment and data.

c. An overview of the DON AIS Security Program will be provided as required. Other training will be provided to ensure all NDCSW personnel have an adequate awareness of AIS security.

10. **Internal Control.** The Management Control Review Coordinator is responsible for ensuring AIS security considerations are included in audits and interval reviews. Audits are conducted in accordance with ref(h). In support of Management Control Reviews, a Security Test and Evaluation (ST&E) will be performed on all the computer systems by the ISSO in coordination with appropriate ADPSSOs. The details of the ST&E will be determined upon the completion of the Risk Assessment (R/A). This method of internal review will be used when major changes are made to the AISs.

11. **Life Cycle Management (LCM).** The Director for Dental Center Administration will ensure that the guidelines and principles as set forth in ref (d) are included in AIS operations and acquisitions and that appropriate AIS security requirements are incorporated into the development and procurement cycles of new hardware/software systems. He/she will assure that AIS security is specifically

27 April 1999

addressed during the LCM documentation process and whenever a previously authorized system configuration is subsequently modified.

12. **Security in Hardware and Software Configuration Control.**

The ISSO will ensure that all necessary features/requirements are evaluated in new hardware/software configurations. No changes will be made to hardware/software for any systems without prior approval of the DAA. Automated System Decision Papers (ASDPs) will be kept on file to reflect the current hardware and software configuration.

a. Microcomputers used at NDCSW are contracted "off-the shelf" hardware. These systems are protected by limited access and properly cleared for "need-to-use" personnel. Modifications are controlled by the DAA, based on documented evidence of a need-to-modify by either the contractor or the user. A description of the Microcomputer equipment is contained in Appendix B.

b. Software

(1) Any changes to the systems will be approved by the DAA and installed by authorized personnel. Operating systems are provided by vendor contract. Application software may be provided by vendor or government resources. Modifications to microcomputer software will be approved by the DAA only after determination that modification does not infringe on copyright laws.

(2) All software and operating systems have backup capabilities, such as tapes, disks, diskettes and printouts.

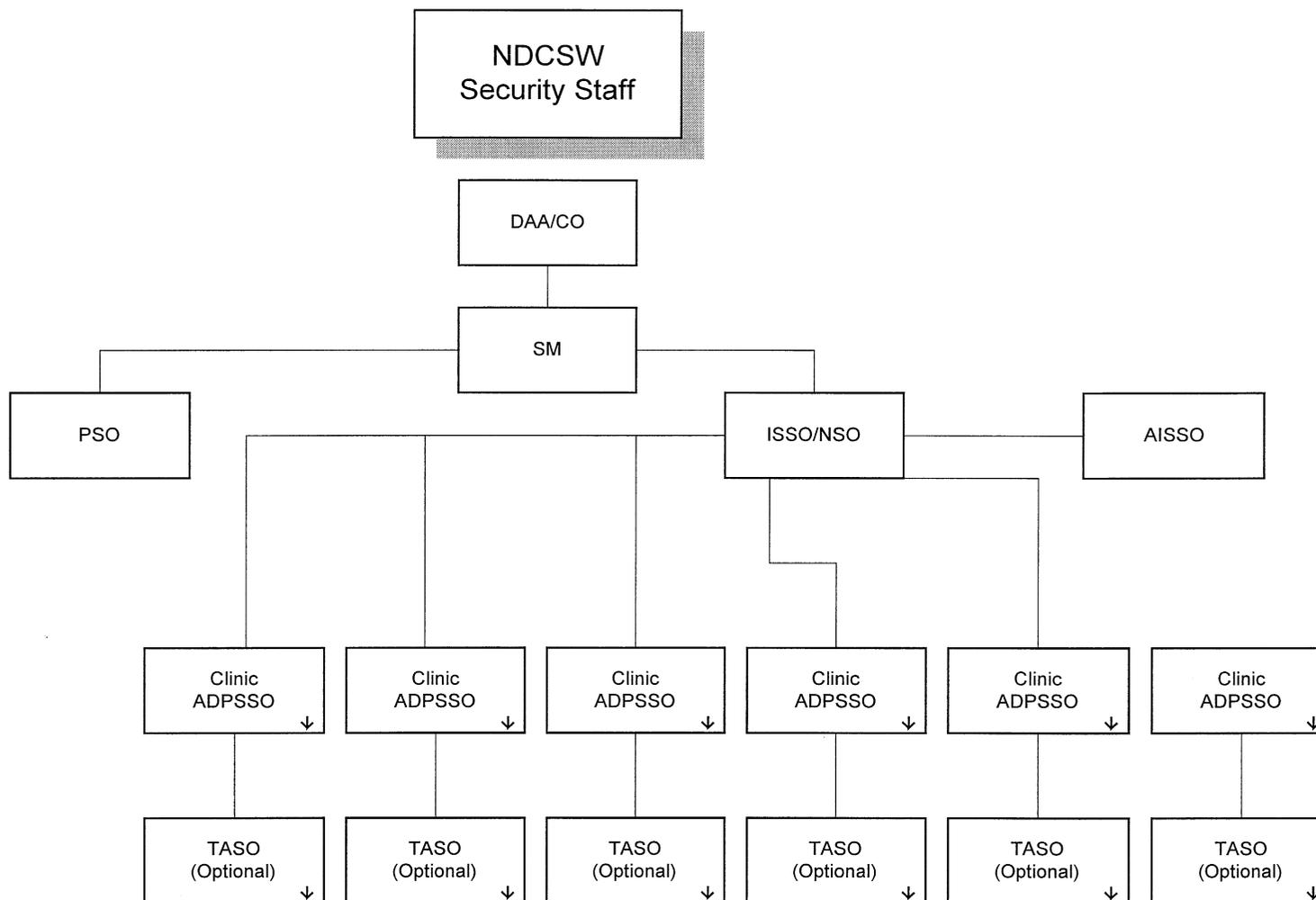
(3) Copyrighted software utilized by this command is listed in Appendix B.

c. Modification to telecommunications equipment listed in Appendix B, requires concurrence of the Network Security Officer (NSO) and the approval of the DAA.

d. Acquisition Requirements. All requests for AIS hardware, software, or services to be reviewed and approved by the Information Systems Executive Board (ISEB). The ISEB will ensure that consideration of AIS security is addressed in each procurement request. The Chairman, ISEB is the Executive Officer who is responsible for acquisition management and the Configuration Control Program as identified below.

13. **Activity Accreditation Schedule (AAS).** Appendix C is the Plan of Action and Milestones (POA&M) to achieve accreditation. The Information Systems Security Officer (ISSO) is responsible to ensure that milestones are met for systems currently onboard and that newly acquired systems are included in the AAS as required. ADPSSO's with input from the TASO's will provide the necessary support in accomplishing the AAS.

APPENDIX A



APPENDIX B

LISTING OF HARDWARE AND SOFTWARE

1. This Appendix contains descriptions of individual system codes with details of the AIS security environment for each, including complete hardware/software descriptions. ADPSSO will advise the ISSO of changes to Appendix B.
2. Primary functions of NDCSW microcomputer systems are used for word processing, spreadsheet analysis, electronic mail, web browsing, and data base management operations. Software is developed and provided by vendors and government. Systems will handle Levels II and III data.

CURRENT INVENTORY LISTING HELD IN MANAGEMENT INFORMATION DEPARTMENT

APPENDIX C

NAVDENCENTER Southwest

Activity Accreditation Schedule

This Appendix contains the Plans of Action and Milestones (POA&M) for FY 99 accreditation. The AIS Security Officer (ISSO) is responsible to ensure that milestones are met for systems currently onboard and that newly acquired systems are included in the NDCSW Activity Accreditation Schedule (AAS) as required. Departments, Divisions, and Sections will provide the necessary support in accomplishing the AAS.

1. Proposed Activity Accreditation Schedule (AAS). The proposed Activity Accreditation Schedule, will be completed.
- 2 Risk Assessment. A risk assessment on NDCSW's AIS will be conducted every three years or whenever major changes to hardware, software, or AIS facilities occur, or other such events which may affect a system's security posture.

PLAN OF ACTION AND MILESTONES

Form Risk Assessment Team	28Dec98
Assign Tasks and Brief Team	29Dec98
Identify Assets by completing AIS Survey for each computer	22Jan99
Conduct AIS Risk Assessments	22Feb99
Identify and Justify Rating of Threats and Vulnerabilities/ Existing Countermeasures	23Feb99
Conduct Standard Test and Evaluation (ST&E)	11Mar99
Correct any Discrepancies Found During ST&E	19Mar99
Formal Presentation to Commanding Officer	27Apr99
Publish Risk Assessment Report	30Apr99

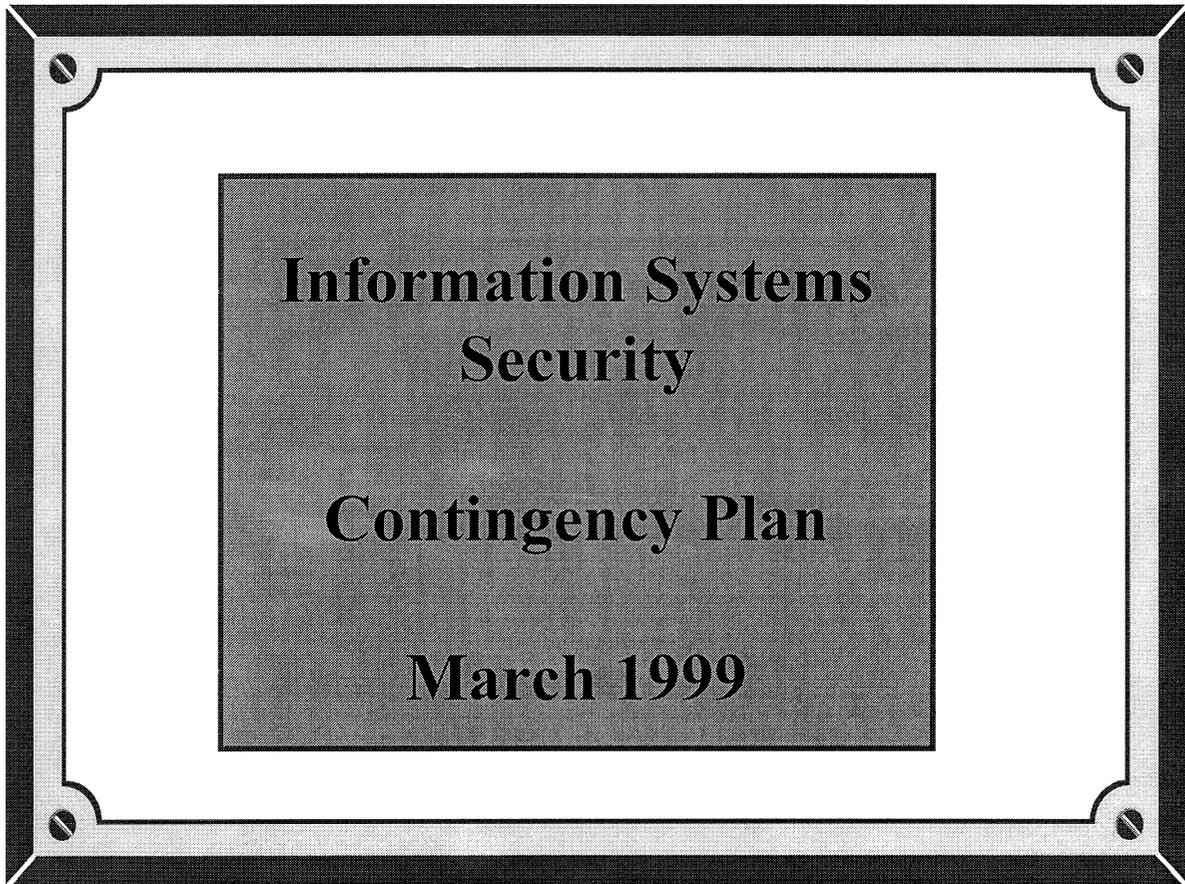


TABLE OF CONTENTS

Paragraph	Page
1. Introduction	3
2. Contingency Reaction Team	3
3. Threats	3
4. General Safeguard Listing	4
5. Emergency Response	4
6. Backup Operations	5
7. Recovery Operations	7

1. **Introduction.** This document has been designed to provide essential guidance for contingency preparations, emergency reactions, backup operations and the restoration of services following the occurrence of a contingency situation for NDCSW (NDCSW) and outlying clinics. This is a working document (guide) to be used in threat scenarios. ADP Security Personnel should be aware of the procedures in this document.

- a. Ensure continuation of the support service of NDCSW in accomplishing the mission/objectives.
- b. Document specific action steps to be followed during or following the occurrence of an unforeseen event.
- c. Provide the necessary resources and procedures for restoring normal conditions.

2. **Contingency Reaction Team.** The command Contingency Reaction Team consists of the Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) and clinic Automated Data Processing System Security Officers (ADPSSO's).

- a. Primary responsibility is to provide action required to prepare the command for implementing a contingency response. Next, is to provide reaction operations which cover the steps following a reduction of loss of processing capability.
- b. During the implementation of a contingency response, ADPSSO's will coordinate with the Emergency Response, Backup Operations and Recovery Operations.
- c. A routine backup program of all data files used on a key computer systems shall be backed up on a weekly basis and maintained at the processing facility to support the Contingency Plan. Each Mission Critical computer has a built in backup utilizing the software. Backup will usually take 30 minutes or more to complete so it should be completed at the end of the day.
- d. A list of critical supplies to support backup operations and facility recovery shall be maintained by the processing facilities ADPSSO's. In addition to logistical arrangements, delivery shall be included as a secondary step.

3. **Threats.** In reviewing the current Risk Analysis the conditions that could significantly affect NDCSW Automated Information System (AIS) operations include, but are not limited to:

- (1) Sudden power failure of unknown duration.
- (2) Minor fires.
- (3) Major power failure, expected duration of three days or longer.

27 April 1999

(4) Major fire that requires backup operations be activated.

4. **General Safeguard Listing**

- a. Ensure windows and doors to computer room are secured against intruders.
- b. Key control. Ensure strict key control is maintained for clinical spaces with AIS equipment.
- c. After hours Clinic Entry. Ensure audit trail is maintained using duty log to reflect who entered the clinic so that responsibilities can be ascertained in the event of a problem.
- d. Escort visitors and maintenance personnel to ensure appropriate behavior.
- e. Maintain computer access through password control. Passwords will be changed on a semi-annual basis.
- f. Challenge with proper ID all personnel attempting to gain access into AIS systems (i.e. I.G. inspector, BUMED Inspection Team etc.).
- g. Every computer and device must have a surge suppressor to avoid any possible electrical damage.
- h. Ensure smoke and fire detectors are tested periodically to ensure they are functioning appropriately.
- i. Fire extinguisher and Tri-Chem systems should be inspected by Federal Fire Department personnel in accordance with OPNAV regulations. Ensure clinic personnel are familiar with the use of fire control equipment to ensure that quick reaction to small fires, thus preventing large fires and injury.
- j. Names of personnel allowed access to the AIS equipment must be strictly enforced.
- k. All AIS equipment and AIS generate media will be labeled identifying the media and indicating the sensitivity and/or classification of the data contained on the media (i.e., unclassified/sensitive, confidential, classified, secret. This command is not authorized to store or produce classified documents with the exception of one computer in the Management Information Department.

5. **Emergency Response.** This section outlines the steps taken immediately after the threat event.

Scenario 1 - Sudden power failure of unknown duration

Emergency Response Procedures/Responsibilities

1. Initiate power down procedures.
2. Notify key personnel, refer to Appendix A.
3. Notify users of disruption of services.
4. Determine whether the situation is localized or wide-spread.
 - If localized, investigate use of other available on-site power.
 - If wide-spread, investigate feasibility of activating backup operations.

Scenario 2 - Fire or Flood

Emergency Response Procedures/Responsibilities

1. Evacuate personnel from building and muster at an assigned area.
2. Notify appropriate agencies:
 - Fire Department
 - Security
3. Initiate power shutdown procedures.
4. Inform management.
5. Assess impact.
6. Initiate protective measures to minimize impact to AIS.
7. Physically secure the area.
8. Inform users of service interruption.

6. **Backup Operations.** This section of the plan contains backup processing procedures to conduct AIS Operations at less than full capacity of the system. The operating procedures for the following events are interim measures that are implemented until full capacity is recovered.

Scenario 1 - Major power failure, expected duration three days or longer

Backup Operations Procedures/Responsibilities

27 April 1999

1. ADPSO notifies alternate facility.
2. ADPSO informs users of service disruption.
3. Processing facility ADPSSO/TASO arranges transportation of personnel and data to the alternate facility.
4. Processing facility ADPSSO/TASO supervises retrieval of backup supplies.
5. ADPSO assembles copies of software and documentation.
6. Processing facility ADPSSO/TASO transports personnel and supplies to alternate facility.
7. ADPSO installs applications on alternate facility.
8. ADPSO tests installation.
9. Restoration of AIS service to users.

Scenario 2 - Fire that necessitates moving AIS operations to off-site facility

Backup Operations Procedures/Responsibilities

1. Evacuate personnel from building and muster at an assigned area.
2. Notify appropriate agencies:
 - Fire Department
 - Security
3. TASO initiate power shutdown procedures.
4. ADPSSO/TASO inform management.
5. ADPSSO/TASO assess impact.
6. Initiate protective measures to minimize impact to AIS.
7. ADPSO notifies alternate facility.
8. ADPSSO informs users of service disruption.
9. TASO physically secures the area.
10. ADPSSO/TASO will arrange for transportation of personnel and data.

11. ADPSSO/TASO supervises retrieval of backup supplies.
12. ADPSO assembles copies of software and documentation.
13. ADPSSO/TASO transports personnel and supplies to the alternate facility.
14. ADPSO installs applications on alternate facility.
15. ADPSO tests installation.
16. Restoration of AIS service to users.

7. Recovery Operations. This part of the plan will only be activated following one or more of the actions described in which backup operations procedures were implemented.

Scenario - Major power failure or fire and off-site backup plan was activated

Recovery Planning Procedures Responsibilities

1. Terminate backup operations.
2. Coordinate transition back to original site.
3. Return backup resources to backup site.
4. Return personnel to normal duties.
5. Resume normal processing operations.
6. Advise users of restoration of normal services.