



DEPARTMENT OF THE NAVY
COMMANDER NAVY REGION SOUTHWEST
937 NO. HARBOR DR.
SAN DIEGO, CA 92132-0058

IN REPLY REFER TO:

COMNAVREGSWINST 5239.1A

N62

26 SEP 2000

COMNAVREGSW INSTRUCTION 5239.1A

Subj: ACTIVITY INFORMATION SYSTEM SECURITY PLAN (ISSP)

Ref: (a) OPNAVINST 5239.1B
(b) SECNAVINST 5239.3
(c) CINCPACFLTINST 5239.3

1. Purpose. To establish, amplify and clarify the Navy Region Southwest San Diego Metro Information System Security Plan (ISSP), to provide guidance in the execution of the ISSP, and to establish the requirements for accreditation of all Regional Information Technology Service Center (RITSC) Information Systems.

2. Cancellation. COMNAVBASESANDIEGOINST 5239.1

3. Background. Reference (a) is the Department of the Navy (DON) Information Assurance (IA) Program, which contains Navy wide policies and procedures for all areas of computer related security. Reference (b) is computer security guidelines setting accreditation policies and Offices of Primary Responsibility (OPRs) for all types of computer resources. Reference (c) is the Pacific Fleet Information Systems Security Program. For the purpose of this instruction the terms, Office Information System (OIS), Automated Data Processing (ADP), Automated Information System (AIS) and Information System (IS) are considered to be synonymous.

4. Objectives of the Information System Security Plan (ISSP) are:

a. Implement an Information System Security Plan, which provide a basis for compliance with references (a) through (c).

b. Ensure all elements of the Information System are adequately protected against accidental or intentional modification, destruction, or disclosure of data and that users are protected against intentional or accidental denial of Information system services in consonance with appropriate level of trust (C2).

5. Scope. The RITSC ISSP establishes command security measures for the protection of all NRSW RITSC computer resources in the

26 SEP 2008

San Diego Metro area. This includes all AIS, including mainframe and mini computer systems, electronic communications systems, word processing systems, personal computers, fax machines and memory typewriters. Commands are required to comply with references (a) through (c) while processing any data, including unclassified information, on CNRSW RITSC computers.

6. Policy

a. The Assistant Chief of Staff for Information Systems is the Designated Approving Authority (DAA) for all NRSW RITSC owned computer resources. The DAA has overall responsibility for all matters concerning computer security within the Southwest Region.

b. All RITSC information systems will operate under reference (a) and this instruction.

c. The DAA will appoint an Information System Security Officer (ISSO). The ISSO will implement command INFOSEC policies.

d. The RITSC Director is responsible for all computer networks in the San Diego Metro area, and will appoint a Network Security Officer (NSO) for each networked computer system. The NSO will report to the ISSO on all matters pertaining to the network system security.

e. The Computer Security Staff, consisting of the ISSO and NSO will continuously monitor the Computer Security Program to ensure adequate security measures are in force.

f. Computer Security Policy is based on the highest classification level of data handled within the command as defined in reference (a).

g. LAN workstations processing sensitive unclassified/classified information shall operate in the DEDICATED mode of operation since all authorized users must have the minimum-security clearance and the need-to-know for all information in the system. All NRSW San Diego Metro unclassified systems are determined to be sensitive but unclassified per references (a) and (c).

h. The use of personally owned PC's within government workspaces is prohibited. The RITSC Director may, when

conditions warrant, grant a waiver. A separate waiver request will be submitted to the RITSC Director, via the NSO, ISSO and will include the following: type of equipment, location and intended purpose. Only non-work related processing may be done on privately owned PC's.

i. All information systems operating within the scope of the RITSC INFOSEC Program will meet the accreditation requirements of reference (a). They will be operated only if:

(1) They are accredited; or

(2) If interim authority to operate (IATO) has been granted in writing by the appropriate designated approving authority (DAA).

j. Each information system must have its own valid copy of software if protected by copyright laws or be under a valid site license agreement. No personally owned software is allowed on government owned or leased computers.

k. All INFOSEC violations shall be reported immediately to the ISSO for immediate action. The ISSO is responsible for keeping the DAA and the RITSC Director informed of such incidents, as well as providing recommendations to resolve these conflicts.

l. The ISSO shall provide annual INFOSEC GMT lectures as well as INFOSEC indoctrination briefs for all newly reporting personnel. All file servers, LAN workstations, stand-alone PC's, and laptops will have the latest anti-virus software installed. When a virus is detected, users are required to notify the NSO. The ISSO is responsible for reporting viruses to Naval Computer Incident Response Team (NAVCIRT).

m. All diskettes (unclassified and classified) will be labeled with the appropriate SF710 classification label.

n. The Controlled Access Protection (CAP) is the minimum set of automated controls that should be provided to DON information systems. "C2" is the CAP level for RITSC computers. The "C2" CAP controls are provided to systems personnel to ensure the requisite level of protection are:

(1) Identification and Authentication. (User-ID, password verification)

6 SEP 2000

(2) Discretionary Access Control

(3) Audit capability

(4) Object Reuse

(5) Contingency Plan (developed, tested and documented for all mission critical systems.)

7. Accreditation is a formal declaration by the Designated Approving Authority (DAA) that a system is approved to operate in a particular security environment meeting a prescribed set of security requirements. This instruction is the prescribed set of security requirements. All NRSW San Diego Metro AIS will operate only if they have been accredited or have an Interim Authority to Operate (IATO). The IATO is not to exceed a period of one year. The ISSO and NSO shall perform accreditation of RITSC information systems. Accreditation consists of:

- a. Computer Survey Forms (Appendix A reference (c))
- b. Risk Analysis Safeguard (Appendix B reference (c))
- c. Security Test and Evaluation (Appendix C reference (c))
- d. DAA accreditation statement (Appendix D reference (c))

8. Information System Security Organization and Responsibilities. The information system security organization and responsibilities are specified below.

a. The DAA shall:

(1) Establish and ensure an Information System Security Program is maintained.

(2) Appoint an ISSO, in writing, as the focal point for activity INFOSEC matters. The ISSO shall have direct access to the DAA on matters relating to INFOSEC via the chain of command.

(3) Formally grant authority to operate an Information System based upon determination that the system will be operated with an acceptable level of risk.

b. The Information System Security Officer (ISSO) is responsible for implementation of the Information System Security Program. The ISSO shall:

- (1) Act as the focal point for all INFOSEC policy and monitor its implementation.
- (2) Develop the Information System Security Program.
- (3) Appoint the Information System Security Staff in writing. Coordinate appointments with the chain of command.
- (4) Obtain authority from the DAA to operate information systems prior to implementation.
- (5) Conduct annual GMT lectures as well as INFOSEC indoctrination briefs for all newly reporting personnel.
- (6) Ensure all computer security incidents or violations are investigated, documented and reported to the Commanding Officer.
- (7) Maintain a current inventory of all CNRSW RITSC computer hardware and software.
- (8) Ensure that virus attacks are resolved and reported to NAVCIRT.

c. The Network Security Officer (NSO) shall be appointed in writing and shall carry out the ISSP for all computer resources within the base. The (NSO) shall:

- (1) Act as the representative for all INFOSEC matters.
- (2) Document, evaluate and report all security problems and risks to the ISSO, assist the ISSO in resolving security problems quickly and effectively.
- (3) Provide assistance to the ISSO in accreditation of information systems, and assist with monitoring, auditing and training.
- (4) Maintain a complete inventory for the base and forward changes to the ISSO.

COMNAVREGSWINST 5239.1A

26 SEP 2000

d. Terminal Area Security Officers (TASO). TASOs are assigned by the NSO. The TASO shall:

(1) Assist NSO in INFOSEC matters as needed.

(2) Document, evaluate, and report all security problems to the NSO.

9. Action. All personnel who use or have access to computer resources shall be familiar with, and comply with the NRSW San Diego Metro contents of this instruction.



D. C. KENDALL

Deputy and Chief of Staff

Distribution:

www.cnrsw.navy.mil/admin/menu.htm