



**DEPARTMENT OF THE NAVY**  
**PERSONNEL SUPPORT ACTIVITY WEST**  
**937 NORTH HARBOR DRIVE**  
**SAN DIEGO, CALIFORNIA 92132-0076**

**IN REPLY REFER TO:**

PERSUPPACTWESTINST 5239.1E

N6

**NOV 27 2002**

PERSUPPACT WEST INSTRUCTION 5239.1E

Subj: INFORMATION ASSURANCE (IA) PROGRAM

Ref: (a) SECNAVINST 5239.3  
(b) OPNAVINST 5239.1A  
(c) CINCPACFLTINST 5239.3  
(d) PERSUPPACTWESTINST 5230.4B

1. Purpose. To establish and implement an Information Assurance (IA) Program for Personnel Support Activity West (PSA) and its detachments and meet the requirements of references (a) through (d).

2. Cancellation. PERSUPPACTSANDIEGOINST 5239.1D

3. Background. Formal Navy policy for IA is contained in references (a) and (b) and directs Commanding Officers to implement a comprehensive IA Program.

4. Scope. This instruction applies to all Information Systems (IS) used within PSA West and its detachments. This instruction will be effective immediately. Deviation from the procedures prescribed herein is prohibited without written approval of the Commanding Officer.

5. Responsibilities

a. The Commanding Officer, as the Designated Approving Authority (DAA), is responsible for:

(1) Developing an IA Program to provide adequate security to protect all systems and ensure compliance with the Department of the Navy (DON) IA Program.

(2) Appointing an Information Systems Security Manager (ISSM) in writing to act as the focal point for all Information Systems Security Program (INFOSEC) matters.

(3) Accrediting all IS for which he/she is the DAA and grant Interim Authority to Operate (IATO) for all systems not accredited. The DAA, as outlined in reference (b), is the official with authority to approve operation of information systems, activities and networks under his/her command.

(4) Ensuring that contract specifications for IS equipment, software, maintenance, and professional service satisfy IA requirements.

b. The Officer in Charge of the Personnel Support Activity Detachment (PSD) is responsible for the implementation of INFOSEC for all IS within their Detachment. The Officer in Charge will:

(1) Ensure that countermeasures and security requirements are implemented within the PSD.

(2) Promulgate the PSA West standard security procedure-governing network and IS operations.

(3) Ensure those security measures and procedures used within the PSDs fully support the security integrity of the network.

c. The ISSM will:

(1) Coordinate with the Command Security Manager on matters concerning IA to comply with references (a) through (c).

(2) Ensure that an Information Systems Security Policy (ISSP) and accreditation schedule are developed and maintained.

(3) Ensure that Information Systems Security Officers (ISSO), Terminal Area Security Officers (TASO), and Network Security Officer (NSO) are appointed in writing where applicable.

(4) Ensure accreditation support documentation is developed and maintained including risk assessment, Security Test and Evaluation (ST&E), and a contingency plan.

(5) Ensure applicable Standard Operating Procedures (SOPs) are established for the PSA West staff and all PSDs.

(6) Ensure all security incidents or violations are investigated, documented, and reported to proper authority (i.e., Command Security Manager, Commanding Officer, CINCPACFLT, NAVCIRT, etc.).

(7) Conduct periodic checks to ensure IA requirements are met. As a minimum, checks will be performed annually or when the command's security posture changes.

(8) Ensure configuration management of all command hardware and software.

(9) Ensure training for all command INFOSEC personnel and users.

(10) Monitor IS procurements for security impact to ensure compliance with security requirements.

d. The Officer in Charge will appoint an ISSO for each Detachment. The ISSO will:

(1) Coordinate with the ISSM all actions on matters concerning INFOSEC.

(2) Assist the ISSM in the development of the ISSP and other supporting accreditation documentation.

(3) Ensure that personnel security procedures are developed and implemented.

(4) Conduct INFOSEC user training and awareness activities under the direction of the ISSM.

(5) Ensure that all INFOSEC incidents or violations are properly investigated, documented, and reported to the ISSM.

(6) Monitor system activity by conducting periodic checks to ensure the security requirements of the systems are met. Review the system and security logs on a daily basis. Report any intrusions, on-line surveys, or probing immediately to the ISSM.

e. The Officer in Charge of each Detachment will appoint a TASO. The TASO will:

(1) Ensure that the information systems are operated, used, and maintained per command ISSP policies.

(2) Ensure that users have the required security clearance and are authorized to perform IS work.

(3) Ensure that all safeguards required to protect IS are in place and functioning as intended.

(4) Assist the ISSO in the preparation of IS security procedures.

(5) Report any security incidents or violations immediately to the ISSO/ISSM.

f. An NSO will be appointed in writing by the Commanding Officer. The NSO will:

(1) Ensure that countermeasures and security requirements are implemented for each node of the network. Ensure a Memorandum of Agreement (MOA) for security is established for each node/terminal located in another activity and implemented before the node/terminal is connected to the network.

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

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

(4) Maintain liaison with all ISSO's in the network.

g. All information systems users and their responsible supervisors will familiarize themselves with the contents of all directives set forth for the network or system being utilized. All users will ensure the following procedures are strictly adhered to:

(1) Terminal operations will be shut down (following proper shut down procedures) prior to securing for extended time periods.

(2) No user will leave a terminal without signing off or ensuring the screensaver is enabled and password protected.

(3) No user will gain access on a terminal by other than his/her own log-on and assigned password when applicable.

(4) All users are responsible for guarding their passwords and ensuring that passwords are not divulged to anyone, including other authorized terminal users.

(5) Users will not attempt to perform any function he/she is not authorized and/or trained to perform.

(6) In the event of a compromise or password failure, the ISSM, ISSO, or TASO will be notified immediately in order that appropriate and timely action may be taken.

(7) Supervisors will notify the ISSM, ISSO, or TASO when subordinates are disqualified as authorized users due to transfer, termination, job change, or other cause.

6. Action. The following procedures will be strictly adhered to:

- a. Adhere to copyright laws and licensing agreements of software vendors.
- b. Privately owned hardware and software are not authorized in command spaces without the prior approval of the Commanding Officer.
- c. Adhere to Internet policy to meet the requirements of references (b) and (c) and as outlined in reference (d).

7. Review Responsibility. The INFOSEC staff will review this instruction annually and when there is a change to the IA posture.

  
CAROLINE B. KONCZEY

Distribution:  
PERSUPPACTWESTINST 5216.1K, Lists I and II