



**DEPARTMENT OF THE NAVY**  
**PERSONNEL SUPPORT ACTIVITY**  
**937 NORTH HARBOR DRIVE**  
**SAN DIEGO, CALIFORNIA 92132-5190**

PERSUPPACTSANDIEGOINST 5510.1A  
Code N1  
5 January 1996

PERSONNEL SUPPORT ACTIVITY SAN DIEGO INSTRUCTION 5510.1A

Subj: COMMAND SECURITY PROCEDURES

Ref: (a) OPNAVINST 5510.1H  
(b) PERSUPPACTSANDIEGOINST 5239.1C

1. Purpose. To promulgate policy and guidance for safeguarding classified information, requesting personnel security clearances and administering the ongoing security education program as required by reference (a). This instruction has been extensively revised and should be reviewed in its entirety.

2. Cancellation. PERSUPPACTSANDIEGOINST 5510.1

3. Discussion. The Commanding Officer, Personnel Support Activity San Diego is responsible for safeguarding all classified information and for the effective management of the Information and Personnel Security Program in its entirety as set forth in references (a) and (b). Each individual, military and civilian, is responsible for compliance with all aspects of references (a) and (b) and this instruction.

4. Program Management

a. Responsibilities

(1) PSA Security Manager. The PERSUPPACT Security Manager serves as the Commanding Officer's advisor and direct representative in matters pertaining to the security of classified information and personnel security. Responsibilities include coordination and regulation of the handling of classified information by PERSUPPACT staff personnel, taking necessary precautions to safeguard and restrict access to classified material to those personnel with the proper clearance and need to know, and providing guidance to the detachment Assistant Security Managers. The full scope of the Security Manager's duties is set forth in reference (a).

(2) Officers in Charge. PERSUPPACT San Diego Officers in Charge (OIC) are responsible for effective management of the Information and Personnel Security Program within their detachments. In administering this program the OIC will follow the guidelines in

5 January 1996

paragraph 2-6 of reference (a). All OICs have the same authority as the Commanding Officer for purposes of granting and recording clearance/access to personnel assigned to their respective detachments, excluding their own. Security clearances for OICs will be issued by the Command Security Manager.

(3) ADP Security Manager. The PERSUPPACT Staff ADP Security Officer is responsible to the Security Manager for the protection of classified information being processed in ADP, and responsible to the Security Officer for the protection of personnel, equipment and related resources. The specifics of the ADP Security program are delineated in reference (b).

b. Security Education Program. The purpose of security education is to ensure that all personnel understand the need to protect classified information and know how to safeguard it. The goal is to develop fundamental habits concerning security so that proper care and discretion is automatically exercised. Officers in Charge are responsible for identifying the security requirements for their detachment, and will ensure that personnel know the security requirements for their particular assignments. Minimum requirements for security education are found in reference (a).

c. Security Violations and Compromise. The Security Manager, Personnel Support Activity, San Diego will immediately be notified in writing of all security violations and possible compromises. Officers in Charge may direct JAG Manual Investigations as appropriate, which will be forwarded to the Commanding Officer for review and disposition.

5. Classification Management. The Commanding Officer, Personnel Support Activity San Diego has derivative classification authority. Commander in Chief, U.S. Pacific Fleet is an original classification authority.

6. Accounting and Control

a. Accountability

(1) Secret. Establish administrative controls for controlling SECRET material. The Officer in Charge will be the only person authorized to sign for and receipt for SECRET material. The Correspondence/Material Control Form (OPNAV 5216/10) will be used to maintain accountability.

(2) Confidential. Although there is no requirement to maintain records of receipt, distribution or disposition of CONFIDENTIAL material, administrative controls will be established to protect CONFIDENTIAL material from unauthorized disclosure.

b. Controls on Reproduction. Commanding Officer/Officers in Charge will establish positive controls to preclude reproduction of classified material. If a situation arises requiring the reproduction of CONFIDENTIAL material, approval will be requested from and be granted by the Officer in Charge, or PSA Security manager. SECRET material is not authorized for reproduction under any circumstances.

c. Storage. Officers in Charge are responsible for safeguarding all classified information within their detachments. All classified information which is neither being used nor under the personal observation of cleared persons who are authorized access, will be stored in an approved security container as prescribed in Chapter 14 of reference (a).

d. Telephone Transmission. Classified information will not be transmitted over the telephone except as may be authorized on approved secure telephone units.

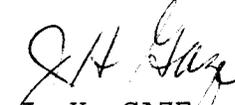
e. DOD Courier Authorization Cards. The DOD Courier Authorization Card (DD Form 2501), is now mandatory for use as the method to authorize handcarry of classified material and information within/outside CONUS. Detachments will implement use of DD Form 2501 in all situations involving handcarry of classified material outside command limits and immediate environs.

f. Destruction. Classified material will be destroyed only by authorized means by personnel cleared to the level of the material being destroyed. Classified material awaiting destruction will be protected according to the information it contains. "Burn bags" will be safeguarded at the level of the highest classification they contain until they are completely destroyed. Burn bags will not be indiscriminately used for trash or other uses. Burning and shredding are the most common methods of destruction.

PERSUPPACTSANDIEGOINST 5510.1A

5 January 1996

7. Personnel Security. Chapters 20-24 of reference (a) should be consulted for detailed information on Personnel Security requirements.

  
J. H. GAZE

Distribution:

PERSUPPACTSANDIEGOINST 5216.1H List II