



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

PERSUPPACTSANDIEGOINST 5530.1B  
Code 21  
28 MAR 1951

FOR OFFICIAL USE ONLY

PERSUPPACT SAN DIEGO INSTRUCTION 5530.1B

Subj: PHYSICAL SECURITY PLAN

Ref: (refer to Appendix A, Section I)

1. Purpose. This plan provides guidelines and procedures to be used for implementing physical security measures at Personnel Support Activity San Diego and its sixteen detachments. This plan defines specific actions required to safeguard assets, prevent unauthorized access, and to protect against unlawful acts, accidents, disasters, etc. This instruction is revised in its entirety.
2. Cancellation. PERSUPPACTSANDIEGOINST 5530.1A.
3. Mission. The mission of Personnel Support Activity San Diego and its components is delineated as follows:
  - a. Personnel Support Activity. To provide logistic support to sixteen Personnel Support Activity Detachments. To provide consolidated pay and personnel service to assigned officer and enlisted naval personnel and passenger transportation service to all Navy-sponsored travelers in a geographic area under the cognizance of a Personnel Support Activity; and to perform such other functions and tasks as directed by higher authority.
  - b. Personnel Support Activity Detachment. To maintain the pay and personnel records, provide pay and personnel service to officer and enlisted naval personnel and passenger transportation service to all Navy-sponsored travelers as assigned by the Personnel Support Activity, to provide commands and activities with pay, personnel and passenger transportation management information and other related support; and to perform such other functions and tasks as directed by the Personnel Support Activity.
4. Applicability. This instruction is applicable to all Navy and Marine Corps, military and civilian personnel employed/located at Personnel Support Activity, San Diego and its sixteen detachments.

  
A. C. SICARI



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

Distribution:

PERSUPPACTSANDIEGOINST 5216.1G, Lists I and II

Copy to:

CINCPACFLT (Code 11)

COMNAVMILPERSCOM (NMPC-08)

Each Host Command's Security Department (16)



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



PERSUPPACTSANDSDIEGOINST 5530.1B



28 MAR 1991

## KEY CONSIDERATIONS

Key considerations in determining the size of the security force include the designation of a qualified Security Officer and the completion of a physical security survey.

Each survey includes a complete reconnaissance, study and analysis of the physical security of each installation's property and its operation. These surveys are designed to show the Commanding Officer what security measures are in effect, what areas need improvements, and provide a basis for determining priorities for funding/work accomplishments. The Security Officer at each activity shall ensure a physical security survey is conducted at least annually. When planning, the following should be accomplished or addressed:

1. Designate in writing a Physical Security Review Committee (PSRC). The committee will:
  - a. Assist in determining requirements for and evaluating security afforded to areas of the activity or installation and its tenant activities.
  - b. Advise on establishment of restricted areas.
  - c. Review draft physical security and loss prevention plans or recommended changes thereto, prior to submission to the Commanding Officer.
  - d. Review report of significant losses or breaches of security and, based on analysis of such instances, recommend improvements.
2. Establish a Physical Security Review Board (PSRB). The board will have functions similar to that of the PSRC, and specifically coordinate mutually supportive physical security and loss prevention practices.
3. Determine the need for existing/new waivers and exceptions to physical security requirements, require employment of compensatory measures/procedures.
4. New construction and facility modifications, when reviewed properly by appropriate personnel and put in place, may require less personnel. The Security Officer must be involved in all phases of new construction or facility modification.
5. Overall importance/criticality of the command.
  - a. Mission and sensitivity of the activity.



28 MAR 1991

- b. Importance of the activity to the continuity of essential naval operations.
6. Overall susceptibility/vulnerability of the command to threats.
    - a. The threat to a specific command as defined by military intelligence and investigative agencies.
    - b. Location, size, deployment and vulnerability of facilities within the activity and the number of personnel involved.
    - c. Need for tailoring security measures to mission critical operating constraints and other local considerations.
    - d. Probable duration of operations.
    - e. Size, geographic location, climate, base population and composition.
    - f. Legal jurisdiction of real property.
    - g. Mutual aid agreements and unilateral assistance agreements.
    - h. Local political climate.
    - i. Adequacy of storage facilities for valuable or sensitive material, including precious metals/drugs and arms, ammunition and explosives.
    - j. Accessibility of the activity to disruptive, criminal, subversive or terrorist elements.
    - k. Possible losses and their impact on command mission and readiness.
    - l. Possibility or probability of expansion, curtailment or other changes in operations.
    - m. Potential for increase in threat.
  7. Number and type of post (how manned and number of hours).
  8. Staff to command, guide and support the force.
  9. Auxiliary security force manning levels, and related post structure, should be sized to protect those assets determined by the Commanding Officer to be critical.





PERSUPFACTSANDIEGOINST 5530.1B  
28 MAR 1991

LEAVE BLANK

28 MAR 1991

TABLE OF CONTENTS

LETTER . . . . . i  
KEY CONSIDERATIONS . . . . . ii  
CHANGES . . . . . iii  
TABLE OF CONTENTS. . . . . v

CHAPTER

1 - CONTROL MEASURES. . . . . 1-1  
- Control Measures . . . . . 1-1  
- Area Security. . . . . 1-1  
- Personnel Identification and Movement Control. . 1-6  
- Admission Procedures . . . . . 1-7  
- Vehicle Identification and Movement Control. . 1-7  
2 - MATERIAL CONTROL. . . . . 2-1  
- Material Control . . . . . 2-1  
- Policy and Procedures. . . . . 2-1  
- Responsibilities . . . . . 2-2  
- Information Material Control . . . . . 2-3  
- Hazardous Material Control . . . . . 2-3  
- AA&E Material Control. . . . . 2-4  
3 - PROTECTIVE LIGHTING . . . . . 3-1  
- Security Areas . . . . . 3-1  
- Systems in Use . . . . . 3-1  
- Inspection and Maintenance . . . . . 3-1  
- Power Failures . . . . . 3-1  
4 - INTRUSION DETECTION SYSTEM. . . . . 4-1  
- Responsibility . . . . . 4-1  
- Standards. . . . . 4-1  
- Maintenance. . . . . 4-2  
- Alarm Response . . . . . 4-2  
- IDS Alarmed Building . . . . . 4-3  
- Emergency Power. . . . . 4-3  
- Continuous Alarm . . . . . 4-3  
5 - PROTECTIVE BARRIERS . . . . . 5-1  
- Physical Barrier . . . . . 5-2  
6 - SECURITY FORCE COMMUNICATIONS . . . . . 6-1



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

7 - SECURITY FORCE. . . . .7-1

- Organizational Chart . . . . .7-1
- Normal Staffing. . . . .7-2
- Records, Reports . . . . .7-2
- Normal Watch Stations. . . . .7-2
- Standard Operating Procedures. . . . .7-2
- Assistant Security Officer . . . . .7-5
- Key Custodian . . . . .7-6
- Key Sub-Custodian. . . . .7-7

8 - AUXILIARY SECURITY FORCE. . . . .8-1

9 - TRAINING SECURITY FORCE/AUXILIARY SECURITY FORCE. .9-1

10 - MOBILIZATION. . . . .10-1

- NAMMOS . . . . .10-2
- Manpower Sources for Mobilization. . . . .10-2
- Manpower Considerations. . . . .10-2
- Annual Validation. . . . .10-3
- EXHIBIT 1 - Mobilization Posts . . . . .10-4
- EXHIBIT 2 - Manpower Summary . . . . .10-5

APPENDICES

A - REFERENCES. . . . .A-1

B - HOST/TENANT SECURITY AGREEMENTS. . . . .B-1

C - MEMORANDA OF UNDERSTANDING,  
INTER-INTRA SERVICE AGREEMENTS. . . . .C-1

D - CRISIS MANAGEMENT ACTIONS, SOPS . . . . .D-1

E - LOSS PREVENTION PROGRAM . . . . .E-1

F - THREAT ASSESSMENTS. . . . .F-1

G - THREAT CONDITIONS . . . . .G-1

H - SAFETY PRECAUTIONS FOR INDIVIDUALS. . . . .H-1

I - RECALL BILL . . . . .I-1

J - PSD SPECIFIC SECURITY REQUIREMENTS. . . . .J-1



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter One:

Control Measures



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Two:

Material Control



28 MAR 1991

## CHAPTER II

1. **Material Control.** Reference (h) requires the controlled movement of government property via commercial and military vans/trucks through the use of the Material Movement Control/Gate Pass (MMC/GP). The use of property passes and car seals as security measures is essential to external security and loss prevention. Every precaution must be exercised to ensure the integrity of government material.

2. **Policy and Procedures:**

a. Procedures for searches and inspections of material during increased THREATCONS are provided in reference (a).

b. Classified shipments will be processed through qualified carriers authorized to transport secret material via a Protective Security Service (PSS) under the Department of Defense Industrial Security Program. Additional station guidelines are found in reference (j).

c. **Property Pass (NAVSUP 155):** The form which authorizes removal of certain specifically described government or private property from a Naval activity through control points and/or access gates. It is the standard form to be used by NAVSTA when appropriate documentation showing proof of ownership or authorization for possession is not with the government or private property. Other typical proof of ownership or authorized documentation is:

(1) Government bills of lading.

(2) Commercial bills of lading.

(3) Adding machine tape annotated "SERVMART" used for all SERVMART purchases.

(4) DOD Single Line Item Release/Receipt Document (DD 1348-1).

(5) Requisition and Invoice/Shipping Document (DD 1149).

(6) Blanket Purchase Authorization (BPA) (NSC 4225/1).

(7) Subsistence Report - Multi-use (NAVSUP 1059).

(8) Material Inspection and Receiving Report (DD 250).

d. **Property Passes:**



28 MAR 1991

(1) A property pass will accompany government property from PERSUPPACT San Diego through any perimeter gate.

(2) Property passes will be picked up by Gate Guards, the Host command Security Police, and other officials who will forward the passes to the Security Officer for return to the issuing department.

(3) If the Host Police, security official, or sentry suspects the authenticity of the signature or entries on documentation or a property pass issued at PERSUPPACT San Diego, they will request the Host command Police to notify the Security Officer and return the holder and property to the originating activity for verification and inspection. Personnel will also be detained if there is a lack of proper documentation or where seal numbers are not annotated on the property pass, if applicable.

### 3. Responsibilities

#### a. Department Heads shall:

(1) Maintain accountability and control over property passes.

(2) Obtain an adequate on hand supply of property passes ensure they are stored in combination lock containers.

(3) Appoint a department custodian (supervisor) to obtain and maintain accountability of property passbooks (including disposition of originals) and return completed passbooks to the Security Officer. Information regarding any suspected usage irregularities in property passes shall be reported to the Security Officer.

(4) Ensure absolute control is maintained over property passes and these items are secured under combination lock at all times, except when in the physical custody of the persons authorized to issue them.

(5) Promulgate internal instructions, as appropriate, to ensure compliance with this instruction. A copy of this instruction should also be furnished to each person authorized to sign property passes.

#### b. Supply Officer shall:

(1) Maintain an adequate supply of property passbooks and control the issue thereof to departments of PERSUPPACT San Diego.

(2) Issue property passbooks to designated departments and Codes custodians and maintain accurate records of these books. Issue records will include passbook serial numbers, date of issue, signature and duty station of person to whom issued.



28 MAR 1991

(3) Review PERSUPPACT San Diego property passes returned; separate and return used passes to issuing departments.

(4) Inspect completed passbooks received from departmental custodians to ensure all returned passes have been matched with the duplicate copy and each missing original has been accounted for by the issuing department. Investigate all matters indicating possible misuse, fraudulent changes, or any other irregularities. Department Heads will be advised of any discrepancies and will be requested to take corrective action.

(5) Periodically review the use and application of property passes to ensure they are being properly utilized.

(6) Establish and maintain liaison between Marine Guard Office, the Host Command Police, and other appropriate officials to ensure property passes issued by PERSUPPACT San Diego departments are returned to this command.

c. Forms Availability: Property pass (NAVSUP 155) is available from I cog stock. Property Pass (NAVSUP 155 dated 7/87) are located in references (e).

4. Information Material Control. Control of classified and privacy act information material is addressed in references (j), (k), and (l). The Security Manager, assisted by the Assistant Security Managers, is responsible for the information and personnel security program; the ADP Security Officer (ADPSO) is responsible for the ADP security program.

5. Hazardous Material Control. Hazardous materials include but are not limited to the following categories: explosives, gases, flammable liquids, flammable solids, spontaneously combustible materials, materials dangerous when wet, oxidizers and organic peroxides, poisonous and etiologic (infectious) materials, radioactive materials, corrosives, and miscellaneous hazardous materials.

a. Handling. All hazardous materials on PERSUPPACT San Diego will be handled in accordance with the following Department of Transportation regulations: 49 CFR 172; 41 FR 42369, September 27, 1976, Revised as of October 1, 1982; 50 FR 46053, November 6, 1985; 50 FR 48419, November 25, 1985; 51 FR 5968, February 18, 1986; 51 FR 23075, June 25, 1986; 51 FR 34985, October 1986; 51 FR 42174, November 21, 1986, effective July 1, 1987, as delayed by 51 FR 46672, December 24, 1987; 52 FR 4825, February 17, 1987; 52 FR 13038, April 20, 1987.

b. Incidents/Accidents. All incidents/accidents involving hazardous material will be handled in accordance with references (m) and Appendix D of this manual.



28 MAR 1991

c. Movement. All movements of hazardous material on PERSUPPACT San Diego shall:

- (1) Be accomplished in approved conveyances
- (2) Conveyances will never exceed 25 miles per hour within station limits
- (3) Conveyances will be escorted by the Host command's Police (Code 2) with one lead vehicle and one follow up vehicle
- (4) Travel to points of destination will be accomplished by the shortest available route
- (5) Conveyances will be inspected at prior to entering/leaving
- (6) The recipients and the Host command's Police will be notified prior to all deliveries/movements
- (7) Movements will not occur during inclement weather (causing unsafe road conditions) or during heavy traffic hours

6. Arms, Ammunition, and Explosives (AA&E) Material Control. AA&E on PERSUPPACT San Diego will be handled in accordance with reference (f); OP-2239, 2139; OP-5, Volume 1; OP-4461, and OP-3681. Movement of all AA&E on PERSUPPACT San Diego will be handled in the same manner as hazardous material addressed in paragraph 5 above.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Three: Protective Lighting



2 8 MAR 1991

CHAPTER III

PROTECTIVE LIGHTING

1. **Security Areas.** Protective lighting is utilized in the following security areas:
  - a. All funds and negotiable instrument storage areas
2. **Lighting Systems in Use.** There are, other than protective lighting for security areas listed above, continuous fixed incandescent and vapor type flood and glare luminaries on the perimeter (mounted on buildings, poles secured to buildings, and on poles). Security areas shall be lighted at all times. Lights are utilized for security, illumination for workers entering and departing during hours of darkness, and for security of supplies and equipment stored on the outside.
3. **Inspection and Maintenance Responsibilities.** DOD security personnel are responsible for the inspection of security lighting with the maintenance under the jurisdiction of the Public Works Department.
4. **Actions to be Taken in Event of Power Failure.** In the event of a commercial power failure, a police unit will be dispatched to the location and the Production Equipment Maintenance Branch, Public Works Department, will be notified and is responsible for the starting of generators and transferring auxiliary power.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Four: Intrusion Detection System



28 MAR 1991

## CHAPTER IV

## INTRUSION DETECTION SYSTEMS (IDS)

1. **Intrusion Detection System (IDS).** IDS are designed to detect, not prevent, actual or attempted penetrations. IDS is useless unless it is supported by a prompt security force response when the system is activated. IDS must contribute to the overall physical security posture and the attainment of security objectives. The IDS system used at PERSUPPACT San Diego is of the proprietary type. IDS systems will be compatible with all terminals at the Host Activity Police alarm panel. The only alarms the NAVSTA Police will respond to are IDS alarms activated at the Host Activity Police Station.

a. **Responsibility.** The following personnel are responsible to ensure a reliable IDS system is maintained:

(1) Security Officer, of the Host Activity. Will provide and monitor the Central Alarm Console located in the Police Headquarters. The Commanding Officer of the host activity is the approving authority for all IDS systems linked to this console.

(2) Commanding Officer of PERSUPPACT San Diego. Is responsible for the proper installation and hook up of all alarms in PERSUPPACT San Diego buildings/spaces/areas. The Host Activity Electronics Division must approve all systems prior to hook up to ensure system compatibility.

(3) Security Officer of the host activity. Is responsible for ensuring user commands follow established procedures in alarm use and will also provide qualified personnel to monitor the Central Alarm Console.

b. **Standards.** The standards for selection concerning installation of IDS alarms will be followed:

(1) The central control panel monitor will provide both a visual and an audible alarm and a specific identifying printout of each protected area. Zone numbers will be used to designate alarmed spaces/areas vice building/room numbers.

(2) All alarm transmission lines between the protected area and the monitor site will be protected by line supervision to detect compromise attempts.

(3) All intrusion alarm systems will provide an alarm signal at the monitoring station when the system is in secure mode and access mode. When in secure mode all alarm equipment is in operation and, when in access mode, all line supervision and anti-tamper switches will be operational.



28 MAR 1991

(4) Key switches used to activate or deactivate alarms will not be installed outside of protected areas. In no case will shunt switches be permitted.

(5) An opening and closing schedule will be developed for each alarm system. The opening and closing schedule will be filed at the host activity Police Headquarters and will state at which time and on which days the activity will normally be opened and closed.

(6) Those high security areas so designated by the host activity Security Officer will be assigned a code procedure to be used whenever changes on an alarm are made. A limited number of personnel will be given a code and they shall communicate via telephone to the host activity Dispatcher giving code, name and activity to prevent potential illegal entry to the activity. A duress code system will be included in these procedures.

c. Maintenance on IDS Systems. Will be performed in accordance with required routine schedules. Emergency maintenance will be performed immediately. The maintenance technicians will test/inspect all systems monthly. This will include testing of the backup/emergency power source. The maintenance technicians will maintain records on all systems to include tests, maintenance, false alarms, etc.

d. Alarm Response. During normal working hours, an attempt should be made to contact the Officer in Charge and, if the alarm is false, direct him to exit the building and inform the on scene patrolmen of the situation. After normal working hours when response to an alarm shows no signs of a burglary attempt, the Duty Section must be called to open and check the building. If an after hour emergency is confirmed and an actual B&E/robbery is taking place as verified by on scene patrolmen, immediately notify the following people:

- (1) Officer in Charge
- (2) PERSUPPACT San Diego SDO

e. IDS Alarmed Buildings. The below listed buildings are alarmed with an IDS system which is linked to an alarm panel located at the Host Activity Police Division Headquarters.

<u>Host Command</u>	<u>PSA Detachment</u>	<u>Bldg No.</u>	<u>Name</u>
FLEASWTRACENPAC SD	PSD ASW	1	Pay Cage
NAVHOSP SD	PSD Balboa	2/Level G	Pay Cage



e. **IDS Alarmed Buildings.** The below listed buildings are alarmed with an IDS system which is linked to an alarm panel located at the Host Activity Police Division Headquarters.

<u>Host Command</u>	<u>PSA Detachment</u>	<u>Bldg No.</u>	<u>Name</u>
R)Kirkland AFB Cage	PSD Albuquerque	926	Pay
FLEASWTRACENPAC San Diego	PSD ASW	1	Pay Cage
R)NAVMEDCEN San Diego	PSD Balboa	2/Level G	Pay Cage
NAVHOSP Camp Pendleton	PSD Camp Pendleton	H-100	RM G233
NAVWPNSTA China Lake	PSD China Lake	02481	Pay Cage
NAB Coronado	PSD Coronado	17	Pay Cage
R)No host command	PSD Denver 13750 E Rice Place Aurora, CO	Suite 100	Pay Cage
NAS Miramar	PSD Miramar	K-175	Pay Cage
NAVSTA San Diego	PSD NAVSTA San Diego	56	Disb Off
NAVSTA San Diego	PSD NAVSTA San Diego	3135	ID Lab
NAS North Island	PSD North Island	515	Pay Cage
NTC San Diego	PSD NTC	94	Pay Cage
NAS PT Mugu	PSD PT Mugu	1	Pay Cage
MCBC PT Hueneme	PSD PT Hueneme	225	Pay Cage

f. **Emergency Power.** An emergency/backup generator is on line to provide uninterrupted power to all IDS's when normal AC power is lost or interrupted.

g. **Continuous Alarm.** All IDS transmission lines, equipment and component housings are alarmed, regardless of mode, 24 hours a day.

# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Five:

## Protective Barriers



28 MAR 1991

CHAPTER V

PROTECTIVE BARRIERS

1. **Physical Barriers.** Physical Barriers control, deny, impede, delay and discourage access by unauthorized persons. Physical barriers will be established around all restricted areas. Perimeter boundaries of all navy installations or separate activities will be either fenced or walled and posted to establish a legal boundary (Reference (a), Chapter 6). The Physical Barriers around PERSUPPACT, San Diego are established and maintained by the Host Activity. PERSUPPACT, San Diego is responsible for internal barriers only.

a. All restricted areas listed in Chapter 1 of this manual are walled and posted to establish a legal boundary.

b. All gates and fencing are the responsibility of the Host Activity.

c. All outside clear zones are the responsibility of the Host Activity.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Six:

Security Force  
Communications



28 MAR 1991

## CHAPTER VI

## SECURITY FORCE COMMUNICATIONS

1. The security force will have its own communications system with direct lines between security headquarters and security elements, an auxiliary power supply and sufficient equipment to maintain continuous 2-Way Voice Communications among all elements of the Security Force. Alternate communications systems are required for use in emergencies to provide for increased communications requirements and to maintain sure and rapid communications throughout the emergency (Reference (a), Paragraph 1000 and Reference (n), Chapter 13). Security force communications is the responsibility of the Host Activity. PERSUPPACT, San Diego has no responsibility in this area except as may be required by the auxiliary security force.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Seven: Security Force





CHAPTER VII

SECURITY ORGANIZATION STAFFING STANDARDS

1. Staffing. The following Security Organization staffing standards are established utilizing criteria set forth in reference (a).

TITLE	MINIMUM # OF COLLATERAL BILLETS	MINIMUM DOD GRADE	MINIMUM MILITARY GRADE
SECURITY OFFICER	1	GS09	E-7
ASSIST SECURITY OFFICER	16	GS06	E-6
KEY CONTROL OFFICER	1	GS06	E-6
KEY CUSTODIAN	17	GS04	E-5
KEY SUB-CUSTODIAN	0	GS04	E-4
TOTAL	35		

2. Records and Reports. Records and reports relating to violations and breaches (including indications thereof) of physical security measures and procedures, including corrective action(s) taken, shall be retained until completion of the command inspection cycle or a minimum of two years, whichever is greater.

3. Normal Watch Stations.

TITLE	DUTY	TOUR OF DUTY	RECALL
SEC. OFF.	IN CHARGE OF SECURITY AT PSA NETWORK	DAYS MONDAY-FRIDAY	RECALL ROSTER
ASST. SEC. OFF.	IN CHARGE OF SECURITY AT PSD	DAYS MONDAY-FRIDAY	RECALL ROSTER
KEY CONTROL OFF.	IN CHARGE OF KEY & LOCK PROGRAM AT PSA NETWORK	DAYS MONDAY-FRIDAY	RECALL ROSTER
KEY CUSTODIAN	IN CHARGE OF KEY & LOCK PROGRAM AT PSD	DAYS MONDAY-FRIDAY	RECALL ROSTER
KEY SUB-CUSTODIAN	IN CHARGE OF KEY & LOCK PROGRAM FOR A FUNCTIONAL AREA	DAYS MONDAY-FRIDAY	RECALL ROSTER



28 MAR 1991

#### 4. Standard Operating Procedures for the Security Organization

a. **General.** The Security Organization provides the enforcement medium for PERSUPPACT San Diego physical security program. This force consists of personnel who are specifically organized and trained to protect the physical security interest of the command. It is the most effective and useful tool in administration of the physical security program.

b. **Security Organization Duties.** Security Organization duties vary with imposed requirements. However, all assigned duties contribute to the physical security program. Security personnel will achieve their purpose by a combination of actions consisting principally of the following:

(1) Operate and enforce the system of personnel identification.

(2) Observe designated perimeters, areas, structure and activities of security interest.

(3) Enforce the established system of control over the removal of property and documents or material of security interest from the installation as may be applicable.

(4) Act as necessary in the event of situations affecting the security of the installation (including fires, accidents, internal disorders and attempts to commit espionage, sabotage or other criminal acts). Provide preliminary or final investigation of criminal acts occurring on PERSUPPACT San Diego.

(5) Generally safeguard information, materials or equipment against espionage, sabotage, unauthorized access, loss, theft or damage.

(6) Report to the Commanding Officer, PERSUPPACT San Diego, through the Security Officer, periodically as a matter of prescribed routine under normal conditions and as necessary in the event of unusual or emergency circumstances.

c. **The Security Officer either personally or through subordinates:**

(1) Is responsible for the planning, development, installation, implementation, administration, training and supervision of a comprehensive security program consistent with command guidelines and those established by higher authority. Serves as the command representative for security matters.

(2) Designs and develops protection systems and devices to ensure the material and facilities are not compromised, sabotaged, subjected to malicious mischief or other forms of willful interference.



28 MAR 1991

(3) Identifies restricted areas.

(4) Conducts a continuous study of crime trends and other information due to continuously changing crime and incident patterns, and adjust the work effort to compensate for trends developing or noted.

(5) Reviews and approves work accomplishment of subordinates.

(6) Refers to United States Code, State Penal Code, State Motor Vehicle Code, Uniform Code of Military Justice, Naval Regulations and station instructions for guidance and interprets and directs their application. An offense can be a violation of federal, state, military law or all three, depending on whether the offender is military or civilian and the location in which the crime is committed.

(7) Consults with operating officials in devising protection systems which provide maximum security with the least interference with the organization's work. Resolves problems of conflict between security requirements and organizational missions.

(8) Prepares and authors correspondence, reports, and directives.

(9) Determines personnel, equipment, material and space requirements for physical security operations and initiates the necessary actions to alleviate problem areas.

(10) Maintains liaison, attends conferences and coordinates on a regular basis through personal contact with agents of host commands, forces afloat, other state, country, and city law enforcement agencies and provides advice on current, sensitive situations (i.e. trends in robbery, burglary, assaults, demonstrations, bomb threats, etc.) and elicits cooperation through tact and diplomacy. This is an extremely important task in that the incumbent represents the command and influences inter-command relationships.

(11) Analyzes work requirements and determines staff resources, equipment and other resources needed to accomplish work assignments and make adjustments among subordinates as deemed appropriate.

(12) Establishes and adjusts long range schedules, priorities and deadlines for regular and special work assignments and coordinates work schedules among subordinates.



28 MAR 1991

(13) Reviews, approves, modifies or rejects changes in functions, structure, staffing levels, etc., proposed by subordinate supervisors and collaborates with higher levels of management in making decisions relating to major changes in work plans or operations.

(14) Reviews and analyzes records and reports of work production, costs, equipment and staff resource utilization to evaluate progress and control or reduce costs; reports progress and resolution of problems in achieving goals and objectives to higher management.

d. Assistant Security Officer.

(1) Implements all Security Standard Operating Procedures (S.O.P.), Instructions and Regulations as promulgated by the Security Officer or higher authority.

(2) Formulates and issues written and/or oral instructions and directives for the Security Officer. Performs internal audits/inspections of Security Organization to ensure proper procedures and techniques are being utilized. Ensures personnel training is adequate to ensure the effective and efficient operation of the organization. Proposes/recommends changes to the Security Officer which will enhance organizational effectiveness. Performs general administrative duties for the Security Officer, and acts for the Security Officer in his absence.

(3) Conducts a continuous study of crime trends and other information due to continuously changing crime and incident patterns, and adjusts the work effort to compensate for trends developing or noted.

(4) Approves/reviews work of subordinates and is responsible for the employment of sound technical procedures in every endeavor.

(5) Refers to United States Code, State Penal Code, State Motor Vehicle Code, Uniform Code of Military Justice, Naval Regulations and Station instructions for guidance and interprets and directs their application. An offence can be a violation of federal, state or military law, or all three, depending on whether the offender is military or civilian and the location in which the crime is committed.

(6) Prepares and authors correspondence, reports and directives.

(7) Determines personnel, equipment, material and space requirements for physical security operations and initiates the necessary actions to alleviate problem areas.



28 MAR 1991

(8) In the absence of the Security Officer, maintains liaison, attends conferences and coordinates on a regular basis through personal contact with host commands, forces afloat, other state, country, and city law enforcement agencies and advises on current, sensitive situations (i.e. trends in robbery, burglary, assaults, demonstrations, bomb threats, etc.) and elicits cooperations through tact and diplomacy.

e. Key Control Officer.

(1) Is responsible for the operation and general function of the PERSUPPACT San Diego key and lock control program. The designated person reports to the Commanding Officer via the Security Officer on all matters of key and lock control and program organization.

(2) Determine location and category of all locks at a given facility.

(3) Determine status of all keys currently in use.

(4) Arranging for all key storage including selecting locked containers, key rings, key tags, etc.

(5) Ensuring that all key storage containers are used properly and in accordance with all directives and instructions.

(6) Recommending areas of high security, medium security, and low security in accordance with OPNAVINST 5510.1, 5530.13, and 5530.14 (see Appendix B).

(7) Recommending areas for possible enclave security/master key use.

(8) Designating Key Custodians as needed.

(9) Recommending lock/core rotation schedules as specified in OPNAVINST 5510.1, 5530.13, and 5530.14 (series).

(10) Recommending locations for code storage and, as available, computer program acquisition for key/lock code control.

(11) Identifying locksmith(s) for use by command.

(12) Developing log procedures and forms for practical daily use that comply with all OPNAV instructions.

(13) Ensuring that key and lock procedures are known throughout the command through educational programs.

(14) Covering all other assignments relating to key and lock control as designated by the Commanding Officer.



28 MAR 1991

f. Key Custodian.

(1) Is responsible to the Key Control Officer for the direction and implementation of the command's key and lock control program.

(2) Conducting quarterly inventory of custodial and sub-custodial key accounts.

(3) Arranging for all key control log books and their maintenance.

(4) Arranging to meet periodically with all Key-Custodians to review key logs, discuss rotation schedules, discuss problems, disseminate command education program information, and answer questions from departments on key and lock problems.

(5) Assisting with and carrying out command policy for key and lock control.

(6) Covering all other assignments relating to key and lock control as designated by the Key Control Officer.

g. Key Sub-Custodian.

(1) Is responsible for all keys assigned by the department head. This may include sub-master keys or change keys. All elements of a good key and lock program must be met by the Key Sub-Custodian, including proper logging of change keys, verification of key usage, monthly key inventories as specified in OPNAV instructions, attendance at monthly meetings with the Key Custodian, and other assigned tasks relating to key and lock control at the department level.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Eight: Auxiliary Security Force



28 MAR 1991

## CHAPTER VIII

## AUXILIARY SECURITY FORCE (ASF)

Each navy installation shall organize, equip, and train its own ASF to prevent disruption by on board civil disturbances, repel or contain overt attack by terrorist or criminal elements and to rapidly restore essential activities which may have been disrupted by civil disturbances, overt attack, natural disaster or other crisis. The ASF will consist of on board nondeploying active duty military personnel sufficient to man all additional security posts required to meet threat condition "DELTA" and sustain this manning level for a period of at least 5 days. The ASF will be under the supervision of the Deputy Security Officer For Operations (Reference (a), Paragraph 0405).

Where Marine Corps Cadres are assigned, they will train the Security Force and Auxiliary Security Force Personnel in ANTI-TERRORISM. At installations where a Marine Officer is assigned to the Security Department, he will be the Deputy Security Officer for operations and will supervise all law enforcement/ASF efforts.

Where Marine Corps Cadres are not assigned, Marine Corps Mobile Training Teams will routinely visit Navy installations/activities to assist in training (Reference (a), Paragraph 0405).

PERSUPPACT, San Diego has no responsibility in the area except to provide members for the Auxiliary Security Force at the direction of the Commanding Officer of the Host Activity.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Chapter Nine:

Training  
Security Force/  
Auxiliary Security Force



28 MAR 1991

CHAPTER IX

TRAINING FOR SECURITY FORCE AND  
AUXILIARY SECURITY FORCE

The effectiveness of a security force is influenced by the quality of its training program. Effective training depends on leadership, proper organization and efficient use of resources. High training standards are essential to enable security force personnel to perform their duties in a professional manner (Reference (a) Paragraph 0901).

This chapter addresses training requirements for three separate physical security and law enforcement programs, namely, basic police/guard training, in-service police/guard training, and firearms training. PERSUPPACT San Diego has no responsibility in this area except as may be required by the Auxiliary Security Force.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



Chapter Ten:

Mobilization



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

CHAPTER X

MANPOWER MOBILIZATION REQUIREMENTS  
PLANNING GUIDANCE

NOTE: THIS CHAPTER WILL NOT BE A GENERIC PLAN BUT RATHER A DISCUSSION OF "MOBILIZATION" AND DOCUMENTATION TO SUPPORT MOBILIZATION REQUIREMENTS.

28 MAR 1991

- REFERENCES:
- (a) OPNAVINST 1000.16F
  - (b) NAMMOS USERS MANUAL (P11-1)
  - (c) COMNAVRESFOR P3060.1B
  - (d) CNO MEMO SER 00/6U30207 OF 15 JUL 86

1. **Navy Manpower Mobilization System (NAMMOS).** NAMMOS is the wartime manpower requirements determination process for activities other than Navy ships or squadrons. It is based upon the premise that a required operational capability in a given wartime environment requires a set of work functions to be accomplished. In turn, these required functions generate workload which can be translated into manpower. Mobilization manpower may satisfy that requirement for national emergencies, as well as war.

2. **Manpower Sources for Mobilization.** There are four basic sources of wartime manpower: active military, Selected Reserve (SELRES), Other Military (O.M.) and civilian.

a. Active and civilian authorizations, reassigned Active, and SELRES may satisfy the majority of "Time-Urgent" manpower (requirements needed at M-Day to M+10 days).

b. Reassigned Active, Other Military (IRR, Fleet/Retired, Standby, etc.), and new hire Civilian/Contractor may satisfy M-day to M+180 day manpower requirements.

c. In a national emergency or crisis, "lower priority" wartime manpower authorizations may be reprogrammed to satisfy critical functions that support the United States National Security Interest.

(1) This programming action may be documented in the activity's Logistics Support Mobilization Plan (LSMP).

(2) This action may be invoked under the Emergency Fleet Augmentation Program (EFAP).

### 3. Manpower Planning Considerations

a. Civilian Billets will not be converted to military billets for mobilization except under unusual circumstances.

b. Additional (ADDU) billets do not define a mobilization requirement. If a wartime billet is improperly coded as an ADDU billet, a manpower change request shall be submitted for appropriate reprogramming action.

c. Additional duty in functions such as Auxiliary Security Force (ASF) do not define a mobilization requirement. If a wartime billet is improperly satisfied by an additional duty billet, a manpower change request shall be submitted for appropriate reprogramming action.

d. Mobilization manpower "quantity" is dependent on the mobilization phase conditions: Phase I and Phase II.



28 MAR 1991

(1) Phase I - (M+1 and M+2 months) Workweek is expanded to 60 hours a week (10 hours a day/6 days a week). See references (a) and (b) of this chapter.

Example: Given a 24 hour/7 days a week manned post, reference (b) states that the position manpower coverage factor is 5.073. In Phase I, given the same 24 hour/7 day a week manning requirement, the position manpower coverage factor is 2.934. If there is a peacetime manning of 4 people to this post, then the required wartime manpower quantity is

$$\begin{aligned} \text{Wartime Quantity} &= 4 \times (2.934/5.073) \\ &= 2.313 \end{aligned}$$

(2) Phase II - (M+3 months and beyond). Workweek is reduced to 48 hours a week (8 hours a day/6 days a week).

Example: Given a 24 hour/7 days a week manned post, reference (b) states that the position manpower coverage factor is 5.073. In Phase II, given the same 24 hour/7 day a week manning requirement, the position manpower coverage factor is 3.927. If there is a peacetime manning of 4 people to this post, then the required wartime manpower quantity is

$$\begin{aligned} \text{Wartime Quantity} &= 4 \times (3.927/5.073) \\ &= 3.096 \end{aligned}$$

4. Annual Validation. Reference (a) requires a periodic validation (at least annually) of all mobilization manpower requirements. This ensures that the proper quantity, quality, and time-phasing continue to satisfy programmed mission objectives and required operational capabilities.

a. Critical billets. Security Officer should identify their critical billets and ensure, through station/TYCOM manpower sections, those billets are appropriately managed to preclude vacancies.

b. Documentation. Exhibits 1 and 2 may be used when developing the mobilization manpower plan of physical security and as the worksheet for manning requests. These forms should be as detailed as necessary to fully support manpower changes.



28 MAR 1991

EXHIBIT 2

MANPOWER SUMMARY

Time Phase	MIL/CIV BA/PA	SR	O.M.	NEW HIRE CIV/CONTRACT
M+DAY				
M+10 DAYS	na			
M+30 DAYS	na	na		
M+60 DAYS	na	na		
M+90 DAYS	na	na		
M+180 DAYS	na	na		
TOTALS				



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



**Appendix A:**

References



## APPENDIX A 28 MAR 1991

## REFERENCES:

- (A) OPNAVINST 5530.14B (DON PHYSICAL SECURITY AND LOSS PREVENTION MANUAL)
- (B) SECNAVINST 5500.4F (REPORTING OF MISSING, LOST, STOLEN, OR RECOVERED (MESR) GOVERNMENT PROPERTY)
- (C) SECNAVINST 5530.5 (SECURITY OF SELECTED SENSITIVE INVENTORY ITEMS - DRUGS, DRUG ABUSE, ITEMS, AND PRECIOUS METALS)
- (D) PERSUPPACTSANDIEGOINST 5530.1B (PHYSICAL SECURITY AND LOSS PREVENTION PLAN)
- (E) PERSUPPACTSANDIEGONOTE 1300 (PHYSICAL SECURITY REVIEW COMMITTEE)
- (F) OPNAVINST 5530.13 (DON PHYSICAL SECURITY INSTRUCTION FOR SENSITIVE CONVENTIONAL ARMS, AMMUNITION AND EXPLOSIVES (AA&E))
- (G) OPNAVINST 5560.10B (STANDARD PROCEDURES FOR REGISTRATION OF NON-GOVERNMENT OWNED VEHICLES)
- (H) OPNAVINST 11200.5B (MILITARY POLICE MOTOR VEHICLE TRAFFIC SUPERVISION)
- (I) OPNAVINST 5585.2A (DON MILITARY WORKING DOG MANUAL)
- (J) OPNAVINST 5510.1H (DON INFORMATION AND PERSONNEL SECURITY PROGRAM REGULATION)
- (K) OPNAVINST 5239.1A (DON AUTOMATIC DATA PROCESSING SECURITY PROGRAM)
- (L) PERSUPPACTSANDIEGOINST 5239.1C (ADP SECURITY PROGRAM)
- (M) DOTP 5800.3 (DOT EMERGENCY RESPONSE GUIDEBOOK FOR HAZARDOUS MATERIAL (INCIDENTS))
- (N) OPNAVINST 5580.1 (NAVY LAW ENFORCEMENT MANUAL)
- (O) NAVPERS 93863 (SMALL ARMS MARKSMANSHIP)
- (P) OPNAVINST 3850.4A (PROTECTION OF DEPARTMENT OF THE NAVY PERSONNEL AND RESOURCES AGAINST TERRORIST ACTS)
- (Q) SECNAVINST 5530.4A (NAVAL SECURITY FORCES ~~ASHORE~~ AND AFLOAT)
- (R) SECNAVINST 5520.3 (CRIMINAL AND SECURITY INVESTIGATIONS AND RELATED ACTIVITIES WITHIN THE DEPARTMENT OF THE NAVY)



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Appendix B:

Host/Tenant  
Security Agreements



28 MAR 1991

APPENDIX B

TENANT COMMAND PHYSICAL  
SECURITY PLANS AND HOST/TENANT  
SECURITY AGREEMENTS

NOTE: Tenant commands will comply with host activity physical security requirements. Host and tenant commands will insure that host/tenant agreements outline complete and detailed physical security responsibilities. Physical security plans for tenant activities on a naval installation will be integrated into the installation (HOST) Physical Security Plan (Reference (a), Paragraphs 0200, 0211C and 0211D pertain).



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



Memoranda of Understanding  
**Appendix C:** Inter-Intra Service Agreements



PERSUPPACTSANDIEGOINST 5530.1B  
28 MAR 1991

APPENDIX C

MEMORANDUMS OF UNDERSTANDING (MOU'S)  
INTRA/INTER-SERVICE AGREEMENTS (ISSA'S)

NOTE: Physical Security of separate activities and installations will be coordinated with other military activities/installations in the Immediate Geographical Area and Local Civilian Law Enforcement Agencies or Host Government Representatives (Reference (a), Paragraph 0204). All MOU'S/ISSA'S should be reviewed by COGNIZANT JAG. Copies of MOU'S/ISSA'S are held on file at PERSUPPACT San Diego.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



**Appendix D:** Crisis Management Actions  
Standard Operating Procedures



28 MAR 1991

APPENDIX D

CRISIS MANAGEMENT ACTIONS  
STANDARD OPERATING PROCEDURES

- A. **Barricaded Captor/Hostage Situation.** PERSUPPACT San Diego will comply with the procedures delineated in Chapter VII of the Host Activity Physical Security and Loss Prevention Plan concerning these situations as applicable.
- B. **Threat Conditions.** PERSUPPACT San Diego shall comply with threat requirements when required in accordance with Chapter VIII of the Host Activity Physical Security and Loss Prevention Plan as applicable.
- C. **Destructive Weather.** PERSUPPACT San Diego will follow the procedures in the Host Activity Destructive Weather Plan when destructive weather threatens PERSUPPACT San Diego.
- D. **Emergency Action Plans.** PERSUPPACT San Diego will comply with the Host Activity Emergency Action Plans as applicable.
- E. **Emergency Relocation.** If an emergency of such magnitude occurs that requires the detachment to relocate, guidelines provided in reference (1) will be followed.
- F. **Fire Evacuation Plan**
- a. In the event of fire:
    - (1) Use nearest fire alarm box or telephone the base fire department.
    - (2) Spread the alarm -- pass the word.
    - (3) All personnel clear the building. Muster outside the building in a designated area.
    - (4) If time permits, close all doors and windows.
    - (5) Use fire extinguishers to extinguish fire, pending arrival of Fire Department.
- F. **Bomb Threat/Detection Procedures.** Personnel receiving a telephonic bomb threat will fill out a Telephonic Threat Complaint (OPNAV Form 5527/8). These forms shall be kept immediately adjacent to office telephones. Immediately notify the Officer-in-Charge or SDO. The OIC or senior person present will direct all personnel to search for the bomb. The following checklist should be completed by the person receiving the telephonic bomb threat.



28 MAR 1991

BOMB THREAT INCIDENT CHECKLIST

When a bomb threat telephone call is received, take the following action:

Keep calm and ask the caller:

1. When will the bomb explode?
2. Where is the bomb right now?
3. What does the bomb look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you plant the bomb?
7. Why?
8. What is your address?
9. What is your name?

Write down the following information as soon as possible:

1. Exact words of the caller.
2. Sex of the caller.
3. Race.
4. Approximate age of the caller.
5. Length of call.
6. Phone number at which call received.
7. Time and date call was received.
8. Callers' voice.

Calm	Crying	Deep
Angry	Normal	Ragged
Excited	Distinct	Clearing throat
Slow	Slurred	Deep breathing
Rapid	Nasal	Cracking voice
Soft	Stutter	Disguised
Loud	Lisp	Accent
Laughing	Raspy	Familiar

If voice is familiar, who did it sound like?

9. Background sounds:

Street noises	Office machinery
Weather sounds	Factory machinery
Voices	Animal noises
PA System	Clear
Music	Static
House noises	Local
Motor	Long distance
Booth	Other



28 MAR 1991

10. Threat Language:

Well spoken (educated)  
Foul  
Taped

Irrational  
Incoherent  
Message read

11. Remarks: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

12. Full name and title of person receiving call:  
\_\_\_\_\_  
\_\_\_\_\_

Make the following phone calls:

1. Host Activity Police Headquarters
2. Officer-in-Charge or SDO of command receiving call
3. Appropriate Superior in Command



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Appendix E: Loss Prevention Program



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

APPENDIX E

LOSS PREVENTION PROGRAM

NOTE: A vigorous loss prevention program is essential at every Navy Command. Missing, lost, stolen, and recovered government property will be reported (Reference (a) Paragraph 0303 and Reference (b)).



28 MAR 1991

A. LOSS PREVENTION PROGRAM PERSUPPACT, SAN DIEGO

1. General. References (b) through (d) detail responsibilities of each command/activity located on PERSUPPACT San Diego that are essential to an effective loss prevention program. The program shall be designed to safeguard resources from theft, loss or destruction by establishing an unacceptable risk of detection and/or apprehension.

2. Responsibilities

a. Commanding Officer. The Commanding Officer, PERSUPPACT San Diego has overall responsibility for physical security matters affecting the PERSUPPACT Network and properties of government agencies with which PERSUPPACT San Diego has agreements to provide such service.

(1) The Physical Security Review Committee (PSRC) will meet in accordance with reference (e).

(2) A Loss Prevention Subcommittee (LPS) consisting of the Internal Review Officer and two other PSRC Members are hereby designated. The LPS will meet quarterly to:

(a) Review and tabulate losses and corrective action taken or pending.

(b) Identify and prioritize those items that have a high degree of susceptibility to theft and pilferage. Establish protective measures designed to secure assigned property with emphasis on higher priority items.

(c) Identify command property accountability, inventory and inspection procedures in an effort to offset losses.

(d) Establish command procedures for timely reporting of missing, lost, stolen or recovered government property in accordance with reference (b).

(e) Identify procedures for internal and external investigative measures, to include procedures for notification to Base Police and requests for Naval Investigative Service investigations. All losses should be researched to determine reasons for and trends of reported losses.

(f) Identify legal, disciplinary and administrative procedures applicable to those found responsible and liable for command losses.



28 MAR 1991

(g) Establish an employee loss prevention education program. The program shall include the command's procedures for preventing property losses and care and protection of resources within the command. This training may be included with other employee security training and shall be conducted annually.

(h) Maintain records until completion of the next Command Inspection or a minimum of two years, whichever is greater.

b. Security Officer. Under the direction of the Commanding Officer, PERSUPPACT San Diego, the Security Officer is responsible for the establishment, administration, and coordination of physical security measures involving the protection of Naval and specified governmental agencies in the PERSUPPACT San Diego Network, their military personnel, employees and dependents. Inclusive in these responsibilities is the implementation of the Loss Prevention Program. The Security Officer will ensure the program is properly established, administered and will make periodic reports on its progress to the Commanding Officer.

c. Officers-in-Charge of PERSUPPACT Detachments. Each OIC of a PSD is responsible for the security of the personal property, equipment, and spaces assigned to that command or members of that command. The OIC of each PSD is responsible for ensuring the integration of PERSUPPACT, San Diego Loss Prevention Program, and the development of an individual command Loss Prevention Program.

d. Assistant Security Officers of PERSUPPACT Detachments. The Assistant Security Officers are responsible to their OIC's for maintaining close liaison with the Security Officer to ensure proper compliance with the PERSUPPACT San Diego Loss Prevention Program, and to provide input from the command for revisions and updates to the plan.

e. Department Heads. Each department head is responsible for the security of the personal property, equipment and spaces assigned to that department or members of that department. Department heads will maintain close liaison with the Security Officer to ensure proper compliance with the program.

## B. PHYSICAL SECURITY REQUIREMENTS FOR SELECTED, SENSITIVE VALUABLE OR PILFERABLE GOVERNMENT PROPERTY

1. The following sensitive/valuable items are in this category.

a. Code "Q" items, drugs or other controlled substances designated as Schedule III, IV or V items, in accordance with 21 Code of Federal Regulations, Part 1308.

b. Code "R" items, a drug or other controlled substance designated as Schedule I or II items in accordance with 21 Code of Federal Regulations, Part 1308.



28 MAR 1991

c. Precious metals, Code "R" items, refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granulation, sponge or wire form.

2. Storage requirements for items mentioned above are found in Chapter 3 of reference (a) and reference (c).

### C. PILFERAGE

1. General. The protection of government property from pilfering is one of the primary functions of each activity attached to PERSUPPACT, San Diego. This function includes protection of supplies and equipment in storage areas, during the issue process, while in transit and during use. Pilferage is probably the most common and annoying hazard with which security personnel and commands should be concerned. It can become such a financial menace and detriment to operations that a large amount of valuable manpower is wasted in investigative, reporting and replacement procedures. It is imperative all military personnel and civilian employees, to include management, understand the potential daily losses. Actual losses depend on such variable factors as type and amount of materials and equipment, and supplies produced, processed and stored at the activity.

2. Profile of Pilferers. There are two types of pilferers which activities must counteract, or at least recognize, so measures may be taken to protect against them. The two types are:

a. Casual Pilferer. One who steals primarily because he is unable to resist the temptation of an unexpected opportunity and has little fear of detection. There is usually little or no planning or premeditation involved in casual pilferage and the pilferer normally acts alone. He may take items for which he has no immediate need or foreseeable use or he may take small quantities of supplies for use of family or friends, or for use around his home. The degree of risk involved in casual pilferage is normally slight unless a very large number of persons are involved.

(1) Casual pilferage occurs whenever the individual feels the need or desire for a certain article and the opportunity to take it is provided by poor security measures. Though it involves unsystematic theft of small articles, casual pilferage is nevertheless very serious, and it may have a great cumulative effect if permitted to become widespread - especially if the stolen items have a high cash or potential value.

(2) There is always the possibility that casual pilferers, encouraged by successful theft, may turn to systematic pilferage. Casual pilferers are normally employees of the installations and usually are the most difficult to detect and apprehend.



28 MAR 1991

b. Systematic Pilferers. One who steals according to preconceived plans and steals any and all types of supplies to sell for cash or to barter for other valuable or desirable commodities.

(1) The individual may work with another person or with a group of people some of whom may be members of an organization in a position to locate or gain direct access to valuable items.

(2) The act of pilferage may be a one time occurrence, or such acts may extend over a period of months or even years. Large quantities of supplies, with great value, may be lost to groups of persons engaged in elaborate planning and carefully executed schemes.

(3) Systematic pilferers may or may not be employees of the installation; if they are not attached to the activity in any way they frequently operate in conspiracy with command personnel.

3. Motivations of Pilferers. The following elements may induce pilfering:

a. Targets of opportunity. This particular element of pilfering is probably the most controllable by each activity. Although you may be able to alter a person's desire for an object through media guides and later his rationalization in the same way, the ability to make an object more difficult to get, and therefore raising the risk factor of getting caught, is the greatest deterrent. The opportunity for theft of an item is decreased by limiting access to the item; maintaining strict inventory for early detection of loss and increased personnel involvement in spotting and preventing loss.

b. High personal need or desire. A person's need for an item can only be offset with serious deterrents. Stiff security measures and the harsh penalties for offenders may convince the individual the cost of obtaining it illegally is far outweighed by the cost of getting caught. The implementation of the above mentioned measures and decreasing access to the item will also directly affect the desire the individual may have for the item.

c. Rationalization of Personal Action. The pilferer may find it easier to take an item if he can rationalize the theft through one of the following:

- (1) Why not, others are doing it?
- (2) It's morally right for me.
- (3) It's not stealing, only borrowing.
- (4) It's so easy to take, nobody must care about it anyway.



28 MAR 1991

4. Decreasing Access. Decreasing access can be achieved through several methods:

a. Each command must perform periodic Physical Security Surveys to detect weaknesses in the command's security system.

b. A strict key control program greatly reduces an individual's ability to gain access to areas containing highly pilferable items.

c. Concentrate security measures on items identified as highly vulnerable to pilfering. Trend analysis may assist the individual commands in this area.

5. Inventory Control. Strict inventory control allows commands to keep a tight control on the location of items and allows early identification of a lost item. This aids an investigation, greatly increasing chances of catching the thief. The casual pilferer is much more likely to take an item he feels may not be missed until long after the actual theft, thus decreasing the chances reliable witnesses or evidence may be found. Therefore all commands, departments, and divisions will be responsible for setting up an asset inventory program for all items which do not fall under an already established inventory system. Checking these inventory control programs will be part of each command's Physical Security Survey.

6. Increased Personnel Involvement. Increased personnel involvement can be accomplished through command educational programs. Commands should educate their personnel to the fact that theft of government property affects everyone (examples: increased man hours due to loss of essential equipment, reduced security assets for protection of private property and housing due to time Police Department personnel must spend investigating thefts, etc.).

7. Summary. The combination of preventative measures, investigative procedures, and reporting and disposition procedures are established to decrease the loss of government property. Implementation and correct operation are the responsibility of each Commanding Officer, department head, and supervisor. Each command and department must maintain a continuing program aimed at educating personnel that rationalizations are false. Periodic Plan-of-the-Day notices, training sessions, posters, and memoranda must be used to emphasize punishments for theft, established guidelines for checking out of government property (especially its removal from the command), and encouragement to turn in offenders. The implementation of the above mentioned measures and decreasing access to the item will also directly affect the desire the individual may have for the item.



28 MAR 1991

D. LOSS REPORTING PROCEDURES

1. General. In the investigation of property losses valuable time, information, and evidence is often lost due to the lack of properly trained personnel in the areas of reporting procedures, initial investigation, and crime scene preservation. Therefore, the following guidelines and responsibilities have been established for use at PERSUPPACT, San Diego.
2. Responsibilities
  - a. Security Officer. Responsible to the Commanding Officer for supervision of required investigations and for providing technical assistance to PSD's in loss reporting procedures.
  - b. Officer-in-Charge. Are responsible for integration of MLSR reporting into their detachment's loss reporting procedures and the development of individual detachment loss reporting procedures.
  - c. Assistant Security Officers. Are responsible for proper supervision of the detachment reporting program and the education of all command personnel in loss reporting procedures.
3. Action. Each detachment will assign an Assistant Security Officer. The Assistant Security Officer will be familiar with proper procedures for reporting losses and preserving crime scenes as well as basic investigative procedures.
4. Notification. Upon notification of a loss within the detachment, the Assistant Security Officer will proceed immediately to the scene of the incident and secure the area. At this point the Host Security Department will be called in to properly secure the crime scene. A quick assessment of the scene will be made to determine preservation needed and the general extent of loss. After identifying property lost, the Assistant Security Officer will have a monetary value check done on the lost property. If material content, monetary value, or sensitivity of lost material meets the MLSR reporting requirements the scene will be secured until notification of NIS has been made and proper direction has been received from them.
5. MLSR Reporting Requirements. Losses of property requiring an MLSR report (see para 7) will be reported to the Police Department within an hour of discovery. Critical information such as nomenclature of the item, and location before loss should be made available at the time the Police Department is contacted.
6. MLSR Incidents. All incidents requiring an MLSR report will be referred to NIS for investigation. This action is independent of the MLSR report. Notification of NIS is the responsibility of the reporting command detachment and NOT the Police Department.



28 MAR 1991

7. Types of property. The following types of property are reportable under the MLSR reporting program:

a. Arms, Ammunition and Explosives (AA&E) \*

- (1) All Category I missiles and rockets.
- (2) All Category I through IV arms.
- (3) Smallest individual unit of issue of ammunition smaller than .50 caliber.
- (4) Individual rounds of .50 caliber and larger ammunition.
- (5) Individual mortar, grenade, rocket and missile rounds.
- (6) Individual land mines, demolition charges and blocks of bulk ammunition/explosives.
- (7) Other items with 10 or more pounds net explosive weight.

b. Precious Metals \*

- (1) Economically recoverable gold, silver, platinum (valued over \$100.)
- (2) Commemorative silver.

(\* Sensitive items must be reported within 48 hours.)

c. Property

(1) Navy

(a) All property requiring completion of Report of Survey (DD Form 200), Report of Discrepancy (SF-364) or Transportation Discrepancy Report (SF 361), that is MLSR.

(b) Value thresholds and time frames established by applicable Naval Supply Systems Command (NAVSUP) instructions (references (a) through (e) of reference (b) apply to MLSR submission.)

(c) Currently all government property, except damaged property, requires MLSR reporting.

(2) Marine Corps. All government property.



28 MAR 1991

8. Reporting Channels. If the applicable NAVSUP instruction requires a DD Form 200 or SF-364 and the property is missing, lost, stolen or recovered, the form, upon completion, shall be submitted through the activity Security Officer as an MLSR report (see enclosure (3) of reference (b) for format and routing). SF-361 shall continue to be routed in accordance with reference (d) of reference (b). Message reports are required in certain cases and shall be submitted in accordance with the guidance contained in reference (b).
9. Instructions for completing the MLSR Report.
- a. Minor property item becomes missing, lost, stolen, or recovered at PERSUPPACT, San Diego.
  - b. PERSUPPACT, San Diego personnel verifies the item is a MLSR reportable item by notifying the Assistant Security Officer or the Security Officer.
  - c. PSD Assistant Security Officer contacts the base police and NIS. Block 10 of DD Form 200 will contain a statement with the date of base police and NIS notification.
  - d. The supply/property personnel completes the DD Form 200 (Report of Survey) then gives it to the Assistant Security Officer. The Assistant Security Officer adds the security related portions to the DD Form 200 to make it a MLSR report. In all cases of ADP equipment, the TASO will commence ADP security reporting.
  - e. The Assistant Security Officer contacts the Security Officer to get a MLSR report number. This number is placed in the upper right-hand corner of DD Form 200 (Report of Survey).
  - f. The Security Officer and the Assistant Security Officer log entry into separate MLSR log books.
  - g. The Security Officer notifies the Executive Officer. In all cases of ADP equipment, the Security Officer notifies the ADP Security Officer also.
  - h. Base police and NIS complete preliminary report. NOTE: If NIS or the base police decline investigative jurisdiction, state this in block 10 of DD Form 200.
  - i. The Assistant Security Officer sends copy of MLSR report with preliminary investigation report to the Security Officer and maintains copy for own MLSR log.
  - j. The Security Officer reviews and maintains copy of MLSR report with preliminary investigation for MLSR log.



k. The Security Officer gives a copy of MLSR report to the PSA Supply and Property Manager to modify the inventory of minor property.

l. The Executive Officer reviews MLSR report and preliminary investigation.

m. Wait for base police and NIS investigations to close.

n. The Assistant Security Officer sends copy of completed investigation to the Security Officer.

o. The Security Officer reviews the MLSR report with the completed investigation report and forwards it for signature.

p. The Executive Officer reviews and signs the MLSR report with the completed investigation report.

q. The Commanding Officer reviews and signs the MLSR report with the completed investigation report.

r. The MLSR report with the completed investigation report is forwarded up the chain of command with a copy to the Security Officer and each of the following commands. Block 18B of DD Form 200 will contain the following addresses.

(1) NAVAL WEAPONS SUPPORT CENTER (CODE 2052)  
CRANE, IN 47522-5020

(2) CHIEF OF NAVAL OPERATIONS (OP-09N)  
NAVY DEPARTMENT  
WASHINGTON, DC 20388-5400

10. MLSR Detailed Instruction. More detailed instruction for MLSR reporting requirements and the proper message format can be found in reference (b).

11. Notification Upon Recovery. When lost or missing property is recovered, all parties concerned will be notified immediately to preclude unnecessary commitment of investigative resources.

#### E. REMOVAL OF GOVERNMENT PROPERTY FROM INSTALLATIONS

1. General. Due to the layout of PERSUPPACT San Diego, government material must sometimes leave the confines of government installations during transfer or delivery procedures. In order to maintain positive control over government materials the following guidelines and procedures will be followed by all personnel attached to PERSUPPACT San Diego.



28 MAR 1991

2. Documentation. When transferring material off the Naval Station, one or more of the following forms will be shown to the gate sentry before departing the station:

- a. Requisition and Invoice/Shipping Document, DD Form 1149.
- b. Order for Supplies or Services, DD Form 1155.
- c. DOD Release/Receipt Document, DD Form 1348-1.
- d. DOD Requisition System Document, DD Form 1348.
- e. Material Inspection and Receiving Report, DD Form 250.
- f. U. S. Government Bill of Lading, Standard Form 1103.
- g. Survey Request, Report and Expenditure, NAVSANDA Form 154.
- h. Failure, Unsatisfactory or Removal Report, NAVAIR Form 3069.
- i. Property Pass, NAVSANDA 155.

3. All government material leaving the confines of the station must be documented by one of the above forms. However, items which are obviously personal property are to be exempt from the Property Pass requirement.

4. Gate Searches. The Commanding Officer, of the Host Activity may require the inspection of vehicles entering or departing his station for stolen government property or contraband prohibited on Naval property. The following procedures shall be used whenever vehicle inspections at a gate are conducted.

a. The inspection shall be specifically authorized in writing by the Commanding Officer, of the Host Activity.

b. Vehicles will be stopped without regard to type of vehicle, its appearance, or the driver but will be selected in accordance with a random numbering system outlined by the Commanding Officer's signed authorization.

c. Vehicles will be safely stopped and engines turned off. Security personnel will identify themselves and state that a search of the vehicle is being conducted. The owner/operator will be asked to step out of the vehicle. Upon discovery of stolen government property or contraband, appropriate further investigation will take place. Otherwise, the vehicle will be allowed to proceed after the inspection.



28 MAR 1991

d. Should objection be raised to the inspection of an incoming vehicle, vehicle will not be inspected. However, such objection will cause exclusion of the vehicle from the station and the revocation of the base driving permit. The owner/operator will be so notified upon his objection to the vehicle inspection.

e. Searches of departing vehicles will be conducted even over the objection of the owner/operator.

#### F. PHYSICAL SECURITY SURVEY

1. General. The Physical Security Survey is designed to identify to the applicable command and the Security Officer what security measures are in effect, what areas need improvement, and to provide a basis for determining priorities for funding/work to be accomplished. A Physical Security Survey differs from an inspection in that a survey is a formal assessment of an installation's property and its operations. Physical Security Survey Checklist is contained in Appendix VIII of reference (a).

2. Survey Time Requirements. A survey of each detachment of PERSUPPACT San Diego will be conducted annually in October. Reports will be retained a minimum of three years or until completion of the cognizant Inspector General cycle, whichever is greater.

3. Responsibility.

a. Each detachment is responsible to ensure their Assistant Security Officer is trained in the proper method to conduct the survey.

b. Security Officer. The Security Officer is responsible to ensure surveys are conducted on time and to maintain survey files.

c. All detachments are responsible for conducting their own surveys and providing a copy to PERSUPPACT San Diego Security Officer.

#### G. TREND ANALYSIS

1. General. The purpose of trend analysis is to gather information in a manner which will show where problems are and where they may lead to next, so that police actions can be planned to meet them. Trend analysis, if managed properly, can greatly benefit all functional divisions of the Police Department. It can combine universal and specific factors with physical evidence to provide information useful in creating specific crime prevention schedules and programs.



28 MAR 1991

## H. LOSS RESPONSIBILITY AND DISCIPLINARY ACTION

1. General. The purpose of this paragraph is to outline responsibility for establishing disciplinary measures in cases of loss and/or theft and to segregate types of action to be taken. To help minimize loss of property and create a standard of disciplinary action, the following legal, disciplinary, and administrative procedures and punishments have been established. Commands are encouraged to prosecute violators to the fullest.

### 2. Responsibilities

a. Commanding Officers/Officers-in-Charge. Commanding Officers/Officers-in-Charge are responsible for the education of command personnel and the internal enforcement of policy and disciplinary measures within their jurisdiction.

b. Security Officer. The Security Officer with help from the Assistant Security Officers will be responsible for station wide dissemination of command policy concerning disciplinary measures to be used in cases of theft, negligent loss or damage to government property. Disciplinary actions taken will be published in the POD along with any other articles of information relating to this subject (cost to taxpayers, wasted man hours, etc.).

### 3. Action

a. Criminal Prosecution. Commands will carefully examine the facts of each case to determine if a definite criminal element is involved and if there is probable cause to warrant referral to legal authorities for criminal prosecution. This prosecution is independent of recoupment or claim action arising from the same incident.

b. Discipline. Personnel subject to the UCMJ may be subjected to action under the Code independent of criminal prosecution or claim action.

c. Claims. In cases where negligent loss is involved, the activity having MLSR or custodial responsibility for the property will contact the Naval Legal Services Office or the Staff Judge Advocate concerning procedures for conducting claim action.

4. Personnel will at all times be vigilant to detect fraud, waste, and abuse of government property.

## I. KEY CONTROL

1. General. The purpose of this paragraph is to establish a key and lock control program aboard PERSUPPACT San Diego. Included



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

within this program are all keys, locks, padlocks and locking devices used to protect or secure restricted areas and activity perimeters, security facilities, critical assets, classified material and sensitive materials and supplies. Not included in this program are keys, locks and padlocks for convenience, privacy, administrative or personal use.

2. Responsibility.

a. Key Control Officer. The Key Control Officer for PERSUPPACT San Diego is responsible to the Commanding Officer via the Security Officer for all security related key control and lock control functions on board PERSUPPACT San Diego.

b. Officer-in-Charge of detachments. Officers-in-Charge are responsible for the installation of the key control program within their activities. They will appoint a Key Custodian and provide names to the Key Control Officer.

c. Key Custodian. Key Custodians are responsible to the Key Control Officer for the handling of keys, related records, investigation of missing keys, inventories and inspections, and the overall supervision of the key control program.

3. Action. Keys for security locks and padlocks must be issued only to those persons with a need approved by the activity Security Officer or Assistant Security Officer. Convenience or status is not sufficient criteria for issue of a security key. The Key Custodian will ensure an access list established by the activity Security Officer is posted beside the key control locker in clear view. All sub-custodians will be aware of the list and will issue keys only to those personnel authorized.

4. Storage. All keys covered by this instruction will be stored in the controlling activity's key locker when not in use.

5. Check out. Personnel checking out a key will first sign a key control log held by the Key Custodian or his designated representative.

6. Key Log. A key log will be maintained with each key locker. When not in use it will be kept under constant control of the cognizant custodian. When no personnel are available to oversee the log, it will be secured in an area qualified to hold classified material. The log will contain information to include: keys issued, to whom, date/time issued and returned, and the signature of the person drawing or returning the key. The controlling log will be checked against the key locker to account for all keys.



28 MAR 1991

7. Key Locker. The locker will contain all applicable keys and their duplicates. An inventory list stating the quantity, applicability, and I.D. number of each key will be maintained within clear view of the locker (preferably taped to the inside door of the locker). The key locker will be closed and locked when not in use. The Key Custodian will maintain the master key for opening the key locker in an appropriate secure place.

8. Spare Keys. No more than one duplicate/spare key will be kept on hand. Duplicates will at no time be checked out to personnel for convenience. Before a duplicate key is checked out the Key Custodian will establish the need for the duplicate and the disposition of the original. All requirements for duplicate keys will be routed through the Key Custodian to Public Works. A record of keys replaced will be kept in the key log book for future reference and review.

9. Lock Rotation. All padlocks and combination locks will be rotated (or have the combination changed, if applicable) at least once annually. A report stating the locks changed, date changed, and personnel performing the task will be forwarded to the Key Control Officer for review.

10. Open Padlock. When the door, gate or other equipment that is intended to be secure is open or operable the padlock will be locked onto the staple, fence fabric, or nearby securing point to preclude the switching of the padlock (by a thief, saboteur or terrorist) to facilitate surreptitious entry.

11. Application. All locks and padlocks used for security applications will meet the minimum military specifications for the appropriate level of security use.

12. Inspections. The Key Control Officer will make semiannual inspections of all detachments to ensure the proper operation of the Key Control program.

13. Tenant Activities. Tenant activity Commanding Officers/Officers-in-Charge, shall enforce internal security in their assigned areas. The Host Activity police will patrol all common areas (streets, roads, parking lots, etc.) and inspect external structures and facilities. All violations will be reported by the Security Department. Department heads will provide a statement of corrective action or completion date of proposed action.



28 MAR 1991

a. All buildings and spaces will be secured at the close of the normal work day and anytime not occupied by assigned personnel. Unnecessary utilities will be secured and all external doors, windows and other openings which could provide access will be secured and locked. Inactive or infrequently used areas (gates, doors, storage areas, etc.) should be locked.

b. Individuals assigned to work in buildings or spaces after normal working hours will ensure all means of access to the area not under their immediate observation are closed and locked. The Police Department must be notified of each incident where mission necessity requires a space to be open and unoccupied.

c. Where there is evidence of possible forced entry into a building or space, the Police Department will be notified immediately. The immediate area will not be disturbed until released by the Host Activity Security Officer or his designated representative.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



## Appendix F: Threat Assessments



28 MAR 1991

APPENDIX F

THREAT ASSESSMENTS

1. **Evaluation.** Based on available information, the command must determine the active short, medium, and long-term threat. The Naval Investigative Service can supply these threat evaluations on request. Such information must be carefully analyzed to determine what additional physical security measures are necessary where physical security requirements are not adequate. The possibility of attempts by terrorist groups, criminals, activists or hostile intelligence operatives to penetrate the security of military installations continues to be a matter of serious concern. Accordingly, the Naval Investigative Service will provide, upon request, an annual area threat assessment through the local Naval Investigative Service Office responsible for counterintelligence support for the activity concerned.

2. **Liaison with Law Enforcement Agencies.** All Naval Investigative Service components maintain close and effective liaison with the Federal Bureau of Investigation and other federal, state and local law enforcement and intelligence agencies and disseminate, by the most expeditious means, known threat information affecting the security of a particular military installation. If a command detects or perceives threat information, the servicing Naval Investigative Service component shall be promptly notified. Follow-up action generally consists of the Naval Investigative Service component attempting to obtain amplifying details/intelligence regarding the perceived threat.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



**Appendix G:**

**Threat Conditions**



28 MAR 1991

## APPENDIX G

## TERRORIST THREAT CONDITIONS (THREATCONS)

## FOR COMBATTING TERRORISM

1. **Introduction.** Information and warnings of terrorist activity against PERSUPPACT San Diego and attached personnel will normally be received from security authorities or through security agencies. Information may come from local police, be received directly by command or agency as a threat or warning from a terrorist organization, or be in the form of an attack.

a. **Threat Information.** PERSUPPACT San Diego will make use of threat information provided by the local Naval Investigative Service.

2. **Purpose:** This outlines common terrorist THREATCONS for PERSUPPACT, San Diego.

3. **Declaration of Terrorist Threatcons and Measure Implementation.** The declaration of THREATCONS and implementation of measures may be decreed by a U.S. command or agency or by the Commanding Officer, of the Host Activity or agency head following receipt of intelligence through official sources or an anonymous threat message. Lateral, as well as, vertical reporting will occur to ensure notice of the THREATCON is given to other potentially affected areas.

4. **Weapons and Ammunition.** This plan includes specific instructions on issuing weapons and live ammunition.

5. **Threat Assessment Guidelines.**

a. **General Guidelines.** The following general guidelines provide for uniform implementation of security alert conditions. Assessment factors are defined as follows:

(1) **Existence.** A terrorist group is present, or able to gain access to a given country or locale.

(2) **Capability.** The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

(3) **Intentions.** Recent demonstrated anti U.S. terrorist activity, or assessed intent to conduct such activity.

(4) **History.** Demonstrated terrorist activity over time.

(5) **Targeting.** Current credible information on activities indicative of preparations for specific terrorist operations.

(6) **Security Environment.** The internal political and security considerations that impact on the capability of terrorist elements to carry out their intentions.



28 MAR 1991

b. Threat Levels. Threat levels are based on the degree to which combinations of the following factors are present:

(1) Critical. Factors of existence, capability and targeting must be present. History and intentions may or may not be present.

(2) High. Factors of existence, capability, history and intentions must be present.

(3) Medium. Factors of existence, capability, and history must be present. Intentions may or may not be present.

(4) Low. Existence and capability must be present. History may or may not be present.

(5) Negligible. Existence and/or capability may or may not be present.

c. Environment. Security environment is considered separately as a modifying factor and may influence the assigned threat level.

d. Limitations. These guidelines apply only to the assessment of a terrorist threat against U.S. or DOD interest.



28 MAR 1991

INTELLIGENCE ESTIMATE - THREAT ANALYSIS

1. Ideally, an intelligence estimate/threat analysis should be a routine, continuous function performed by the Host Activity Commanding Officer.

2. Questions to be considered:

a. Is the area ripe for terrorism?

b. Are terrorist groups forming and, if they are, are they becoming violent?

c. Are acts of terrorism likely to happen here?

d. What are the likely targets on this installation?

3. U.S. Government agencies acting as excellent sources of information include the Federal Bureau of Investigation, which is responsible for dealing with terrorism involving military personnel. The Naval Investigative Service will provide liaison between U.S. Navy assets and other government agencies.



28 MAR 1991

VULNERABILITIES

1. The following are PERSUPPACT San Diego vulnerabilities:
  - a. Communication lines and facilities
  - b. Equipment warehouse
  - c. Computer facilities
  - d. PWC transportation
  - e. Logistic and storage facilities
  - f. Command/sensitive cargo storage areas
  - g. Classified/sensitive cargo storage areas.
  - h. Storage facilities - general cargo
  - i. Banking and financing facilities.
  - j. Intrusion detection system monitor stations (Security)
  - k. Motor pools
  - l. Water sources
  - m. Personnel
2. Facility engineer will provide the Command Control Center with floor plans diagrams/blueprints, as required.
3. An Installation Vulnerability Determination System may be used to help forecast the threat of terrorism.
  - a. Factors
    - (1) Installation's characteristics and its attractiveness as a target for terrorist acts.
      - (a) Consider who are hostage candidates.
      - (b) Sensitivity of installation mission.
      - (c) Is the installation considered a symbol of nation or international significance?



28 MAR 1991

- (2) Law enforcement resources
  - (a) Security Department
  - (b) Naval Investigative Service
  - (c) Auxiliary Security Forces
- (3) Distance from population centers - miles/time
- (4) Size of the installation - area population
- (5) Routes to and from installation
- (6) Attitude of area population
- (7) Proximity of boundaries - jurisdiction
- (8) Distance from other U.S. Military Installations - support
- (9) Terrain.
- (10) Availability of communication with next higher command.

No factor should be determined singly. The relationship between factors must also be considered.

5. **THREAT CONDITIONS.** Threat Conditions will be implemented by the Host Activity in all cases. PERSUPPACT San Diego will comply with all directives issued by the Host Activity in this matter.

a. **THREATCON ALPHA.** This condition is declared as a general warning of possible terrorist activity, the nature and extent of which is unpredictable, when the circumstances do not justify full implementation of the measures of THREATCON BRAVO. However, it may be necessary to implement selected measures from THREATCON BRAVO. The measures in this threat condition must be capable of being maintained indefinitely.

(1) Measure 1. At regular intervals, remind all personnel, including dependents, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Be alert for unidentified vehicles on, or in the vicinity of, the Host Activity and be alert for abandoned parcels or suitcases or any unusual activity.

(2) Measure 2. Keep the security officer or other appointed personnel who have access to plans for evacuating buildings and areas in use and for sealing off any areas where an explosion or attack has occurred. Keep key personnel who may be needed to implement security plans on call.



28 MAR 1991

(3) Measure 3. Secure buildings, rooms, and storage areas not in regular use.

(4) Measure 4. Increase security spot checks of vehicles and persons entering the Host Activity and unclassified areas under the jurisdiction of the Host Activity.

(5) Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

(6) Measure 6. As a deterrent, apply one of the following measures from THREATCON BRAVO individually and randomly:

(a) Secure and regularly inspect all buildings, rooms and storage areas not in regular use. (Measure 14)

(b) At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages. (Measure 15)

(c) Check all deliveries to messes, clubs, etc. Advise dependents to check all home deliveries. (Measure 17)

(d) As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrents and defense and to build confidence among staff and dependents. (Measure 18)

(7) Measure 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of the next higher THREATCON.

(8) Measure 8. Review and implement, as appropriate, security measures for high risk personnel.

b. THREATCON BRAVO. This condition is declared when there is an increased and more predictable threat of terrorist activity even though no particular target has been identified. Measures must be maintainable for weeks without undue hardship, operational hindrances or strained relations with local authorities.

(1) Measure 10. Repeat Measure 1 and warn personnel of any other form of attack to be used by terrorists.

(2) Measure 11. Keep all personnel involved in implementing anti-terrorist contingency plans on call.

(3) Measure 12. Check plans for implementation of the measures contained in the next THREATCON.



28 MAR 1991

(4) Measure 13. Where possible, cars and such objects as crates, trash containers, etc., are to be moved at least 80 feet (25 meters) from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

(5) Measure 14. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

(6) Measure 15. At the beginning and end of each workday, and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

(7) Measure 16. Examine all mail for letter or parcel bombs. (This examination is increased above normal.)

(8) Measure 17. Check all deliveries to messes, clubs, etc. Advise dependents to check all home deliveries.

(9) Measure 18. As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents.

(10) Measure 19. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

(11) Measure 20. At an early stage, inform members of local security committees of any action being taken and why.

(12) Measure 21. Upon entry of visitors to the command, physically inspect them and a percentage of their suitcases, parcels, and other containers.

(13) Measure 22. Wherever possible, operate random patrols to check vehicles, people, and buildings.

(14) Measure 23. Protect off base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive a car.

(15) Measure 24. Implement additional security measures for high risk personnel, as appropriate.

(16) Measure 25. Brief personnel who may augment guard force on use of deadly force.

(17) Measure 26. Provide increased security surveillance of waterfront areas including wharfs, piers, caissons, etc., as appropriate.



28 MAR 1991

c. THREATCON CHARLIE. This condition is declared when an incident occurs or intelligence is received indicating that some form of terrorist action is imminent. Implementation for more than a short period will probably create hardship and affect the Host Activity peacetime operations.

(1) Measure 27. Continue all THREATCON BRAVO measures or introduce those outstanding.

(2) Measure 28. Close for business all nonessential activities/functions (i.e., all clubs, exchanges, commissaries, recreational services, etc). All military personnel will be re-assigned as necessary.

(3) Measure 29. Limit access points to absolute minimum.

(4) Measure 30. Strictly enforce control of entry and search a percentage of vehicles.

(5) Measure 31. Enforce centralized parking of vehicles away from sensitive buildings.

(6) Measure 32. Issue weapons to guards. The Host Activity has specific orders on issuing ammunition and weapons.

(7) Measure 33. Introduce increased patrolling of the installation to include waterfront areas, wharfs, piers, caissons, critical communications facilities, drydocks, etc., as appropriate.

(8) Measure 34. Protect all designated vulnerable points (VPs) and give special attention to VPs outside the Host Activity.

(9) Measure 35. Erect barriers and obstacles to control traffic flow.

d. THREATCON DELTA. This condition applies in the immediate area where a terrorist attack has occurred or when intelligence is received that terrorist action against a specific location is likely. Normally this THREATCON is declared as a localized warning.

(1) Measure 36. Activate the ASF and man all designated posts.

(2) Measure 37. Continue or introduce all measures listed for THREATCON BRAVO and THREATCON CHARLIE.

(3) Measure 38. Augment guard and/or police forces as necessary.

(4) Measure 39. Identify all vehicles already on the installation within operational or mission support areas.



28 MAR 1991

(5) Measure 40. Search all vehicles entering the Host Activity as well as vehicle's contents.

(6) Measure 41. Control all access and implement positive identification of all personnel.

(7) Measure 42. Search all suitcases, briefcases, packages, etc., brought into the Host Activity.

(8) Measure 43. Take measures to control access to all areas under the jurisdiction of the Host Activity.

(9) Measure 44. Make frequent checks of the exterior of buildings and of parking areas.

(10) Measure 45. Minimize all administrative journeys and visits.

(11) Measure 46. Consult local authorities about closing public (and military) roads and facilities that might make sites vulnerable to terrorist attack.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



**Appendix H:**      **Safety**  
                                 **Precautions for Individuals**



28 MAR 1991

APPENDIX H

SAFETY PRECAUTIONS FOR INDIVIDUALS

No one is immune to international terrorist threats. A person trained in terrorist acts can minimize and prevent such acts. For this reason, everyone must develop a security conscious attitude. Individuals and members of their families can do a great deal to protect themselves. The following precautionary measures are suggested:

-- Members and their families must know the threat, their role, the protection plan and what to do in an emergency.

-- Everyone must try to avoid routine roads, certain times for going to and from work and even avoiding the same restaurant a second time in a row. Consider varying methods of transportation and style of dress. Past incidents show the attackers keep victims under surveillance for long periods of time to learn travel patterns and to arrange a suitable time and place for the kidnapping or assassination. Keep the office and family aware of your going and coming. Get in the habit of "checking in" before departing and after reaching your destination. Report any unexpected changes. Do not regularly go to work or visit the office when no one is present.

-- Avoid going out alone for any reason. Travel in a group - there is safety in numbers.

-- If possible, travel to and from work or on long distances in a convoy. In a convoy, vary the order of organization and the route used. If a convoy is not possible, consider a small car pool as traveling alone makes one an easy target.

-- Vary the order, time of pickup, and land route to and from work when in a car pool.

-- Insofar as possible, travel only on busy, well traveled thoroughfares and away from isolated country roads. Know and avoid the dangerous areas in the city.

-- Use the center lane when driving on a multiple highway to make it difficult for the car to be forced to the curb or to be attacked from the driver's side - the most common direction of attack.

-- When traveling by car, keep all doors locked and the windows closed or opened slightly.



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

-- Avoid cars or actions that could easily identify you as an American, someone rich, or of importance. Drive a native car and of a popular color.

-- Park the car on well lit streets at night.

-- Lock unattended cars, even for a short time.

-- Inspect for suspicious objects or unexplained wires or strings inside or underneath the car before entering.

-- If suspicious wires or packages are found in the car, office, or residence, report them immediately to the proper authorities. Do not attempt to remove any such objects.

-- If riding in a taxi, do not let the driver deviate from known and desired routes. Do not use the same taxi or take the first available cab. Buses are preferred to taxis but vary bus stops used.

-- Be sensitive to the possibility of being watched. Before leaving the area, check the street for suspicious cars or individuals.

-- Be aware of the chance of being followed to and from work, or to other places. Notify police if it is a possibility.

-- If being followed, move as quickly as possible to a protected place such as a police station, then report the incident, and, if possible, identify the vehicle or person. Ask police to check it. Inform the security officer of the incident.

-- Individuals should not carry a concealed gun unless it is legal and registered. Be sure those who are carrying arms are trained in their use and practice safety procedures. A gun should not be used unless it is a life or death situation. This is to prevent unwanted incidents that may degrade mission performance.

-- Tear gas pens, or other protective devices should be used with caution. They may enrage an attacker instead of rendering them helpless. Training is necessary in the use of such special items.

-- Avoid any civil disturbance disputes with local citizens. If there is a dispute, or an accident, call the local police immediately.

-- Stay away from high risk areas except in line of duty.

-- Keep reasonable amounts of well concealed negotiable money for emergency use.



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

- Do not attend the same night clubs or restaurants or participate in activities such as movies, golf, or tennis on a regular basis.
- Social events should be held in secure areas and with limited invitation.
- Shun publicity by not reporting social gatherings.
- Do not permit your photograph to be taken for unofficial dissemination.
- Safeguard home address, telephone number and information about the family.
- Members not knowing the language of the host country should learn certain key phrases: "I need a policeman," "Take me to a doctor," "Where is the hospital?" "Where is the police station," and "Help!"
- Everyone must know how to use a local commercial telephone in case of an emergency.
- Know emergency telephone numbers such as: police, fire, embassy, security officer.
- Exact change for a pay telephone should always be carried for emergency use; telephone booths may offer refuge against some form of violence while calling or waiting for assistance.
- U.S. personnel should pick up and process all mail to prohibit censoring and to detect suspicious letters or packages for bombs. Mail received from foreign countries through a US facility should be checked electronically for possible bombs.
- Do not habitually take periodic recreational or conditioning walks near the home or office on a set schedule. Vary the time and place when taking a walk. Avoid walking on country roads or on deserted streets; the safest place is in a well populated area and at the height of rush hour. When walking to and from work, use different routes and vary times of departure and arrival. If possible, use several differing entrances and exits.
- Do not dress in a style that would point you out as an American or as a U.S. Government official.
- Do not accept unsolicited packages. Have the carrier open it at some distance.



PERSUPFACTSANDIEGOINST 5530.1B

28 MAR 1991

-- Do not habitually stand by open windows, especially at night with a light in the background.

-- Always carry identification papers. Carry a card stating your blood type and any allergies to medication. The card should be in English and in the language of the host country.

-- Suspect unexplained absences of local citizens as an early warning of possible terrorist action.

-- Travel plans should not be discussed within hearing distance of those not involved. Do not leave travel plans or related papers where others can read them.



28 MAR 1991

## SPECIAL PRECAUTIONS FOR WOMEN

The following are suggestions to prevent criminal activity. These actions collectively will make it difficult for a terrorist to attack. When followed, they increase the atmosphere and structure of security.

-- When Shopping. Never leave a purse unattended in a shopping cart or on a counter. When asked for identification, give only the information requested. Never give your entire wallet or card case. Do not display large amounts of money. Check credit cards at times and immediately report it if any are missing. Keep a record of all account numbers and the company addresses to quickly report lost cards. After making large purchases, check to see if you are being followed after leaving the store.

-- When Driving. Search the car before getting in - an attacker may be waiting for you. Keep the gas tank full. Keep the windows rolled up and doors locked. Park in a well lighted area near your destination. If being followed, blow horn repeatedly to attract attention and drive directly to a safe place. If the car breaks down, raise the hood and trunk, stay inside with doors locked and windows up until police arrive. Tell anyone who offers help to call the police. Don't pick up hitchhikers. Drive only on well lighted streets at night if at all possible, even if it means going out of the way.

-- When Walking. Walk on well lighted, heavily traveled streets. Avoid cutting through alleys. Walk in the middle of the sidewalk. Hold your purse under the arm, with the latch on the inside. Be prepared to run if followed. Walk into a store or police station and report the incident; attempt to identify the individual. If you are approached by a suspicious person, cross the street or change direction. If threatened from a car, run in the opposite direction to seek help. Wait at a well lighted bus stop for the bus. Observe fellow passengers. If frightened, sit near the driver.

-- In An Office Building. Use an elevator where possible. Do not risk being attacked in a poorly lit stairwell. Stand next to the control panel in elevators. If threatened, punch alarm button. Never leave keys or valuables in coat pockets. Use discretion in revealing personal plans to others. If working, keep your purse locked in desk or file cabinet. When working late, tell the building security officer so you can be expected in the lobby. Report suspicious persons or actions in your building to the security officer or supervisor.

-- If Attacked. Scream as loudly as possible. Strike back quickly and aim for vital spots; gouge eyes with thumbs, scratch



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

with fingernails; scratch across the face with a key or fingernail file; hack temple, nose and Adam's apple with purse or book; jab knee into the groin; stomp down on instep, kick shins; grab fingers and bend back sharply; and poke umbrella, comb, fist, or elbow in midriff. Report incident as soon as possible. At work, notify the security officer in the building, or the local police, as appropriate. At home, report incident to the security officer and the local police. Give a good description of an attacker including color of hair and eyes, build, scars or tattoos, height, weight and complexion. It is important to report all incidents. Failure to report the incident may result in others getting attacked.



2 8 MAR 1991

FAMILY SECURITY PROCEDURES

Wives and children are seldom direct targets of terrorists attack although there have been casualties involving family members. Families must be aware they can help prevent terrorist activity and criminal acts through their protective efforts and can contribute to defense if they are security conscious and prepared to act in any emergency. This means they must be briefed and re-briefed on security precautions and be kept informed on any change in threats. Family related security precautions which might be adopted to lessen the probability of successful terrorist activity are as follows:

-- Make sure the family is totally familiar with security procedures and techniques discussed elsewhere in this publication. Prepare them mentally for quick action in case of incident.

-- All family members should know security telephone numbers in case of an emergency and be shown how to use local telephones. This may require learning key phrases in the language of the host country.

-- Be sure the family knows where each member is at all times. Get in the habit of "checking in" before departing or arriving, or when there is a change in plans. This is vitally important to all concerned.

-- Have the family avoid crowds and disturbances and to stay away from high risk areas when they have no meaningful business there.

-- Family members must know they should not become involved in disputes with local citizens. If local citizens start an incident, leave the scene as quickly as possible and report the matter to the authorities.

-- If an accident involves local citizens, call police as soon as possible.

-- All family members must be alert to the known signs of surveillance being done by terrorists, or to any other potentially dangerous occurrence. All questionable happenings should be reported and checked immediately.

-- Anonymous phone calls, threats, or any unusual occurrence should be reported immediately.

-- Family members must be warned not to reveal travel plans, not even to friends, if it can be avoided. Avoid answering questions over the telephone, even if the caller is known, because of the possibility of wiretaps or other leaks.



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

-- Wives and perhaps older children, should carry sonic emergency warning devices such as whistles or air driven claxons to signal for help in the case of attack.

-- Shopping or family outings should not follow any pattern.

-- Discuss with the family what steps to take in case of kidnap or if a victim of other possible attacks. Your organization should be prepared to give support to the family in case of kidnap. They should be told who to see and what support to expect.

-- Children, particularly, must be on guard about being approached or questioned by strangers.

-- Do not permit unaccompanied children to travel in taxis.

-- Although children must attend school on a particular schedule, ensure departures, arrivals and routes are varied. Use car pools, particularly when scheduled on a random basis which breaks the pattern of movement and improves security.

-- It is safer for children to be driven to school instead of having them walk.

-- If riding a bus, children should at least be escorted to and from the bus stop. Private, rather than public, transportation is favored.



28 MAR 1991

## RESIDENCE SECURITY

A survey should be conducted on all residences to determine their security risk. A survey should be conducted and reacted to before a house is occupied. The basic purpose of the survey is to find out if the house is as burglar proof as possible. Security at each residence is to prevent actual penetration of the house or apartment. The specific preventive procedures to complement the protective equipment selected include the following:

-- Residences should be clustered in one general area or neighborhood for mutual support purposes and to ease security problems. Consider areas that are also used by other groups or organizations and have security protection. The house should be near neighbors so a claxon warning or other emergency signals can be heard for quick relay to security forces. This makes it more difficult for terrorists to make the needed reconnaissance, penetration for attack and withdrawal.

-- Select, if possible, an area that has good fire fighting facilities.

-- Find out if the local police patrol the area. If not, request they patrol.

-- Watchdogs have proven to be a major deterrent to terrorists and ordinary criminals; even a timid dog is a prevention. Consider having a dog inside and one outside of the house to provide audible early warning of intruders.

-- Be alert to persons disguised as public utility crews, road workers, vendors, etc., who station themselves near the house to observe your activities and collect information to plan an attack. Note the license number of any suspicious vehicle and the description of occupants. Report such incidents to your superior, the security officer, or the local police as is appropriate for action.

-- Be aware of peddlers, strangers and so-called inspectors or investigators who unexpectedly seek entry to your quarters or its grounds. Do not allow anyone who is not known or expected, to enter the house, no matter how official their credentials or uniform may appear.

-- Select and prepare an interior "safe room" to use as an area in case of attack. It should not be easily accessible from the outside and should have a sturdy door with a lock and an emergency exit if possible. Upper story bathrooms work well for this purpose. A radio, first aid supplies and possibly a telephone should be located in this room.



28 MAR 1991

-- Emergency items such as a supply of fresh water, food, candles or lanterns, flashlights, extra batteries, blankets, portable radio, camping stove with spare fuel, ax, and a first aid kit should be kept on hand. Refrigerators should be kept at a high setting so food can be kept longer in case of power failure.

-- If the home is equipped with an emergency radio transmitter on a protective network, every member must know the code word call signs and how it is to be operated. The radio transmitter should be kept in a secure place; ensure servants do not tamper with the set. A decision will have to be made as to whether to train servants in its operation. Ensure children are taught how to use the radio transmitter; they are often ignored during serious incidents and perhaps can give a warning.

-- All household members should have emergency telephone numbers and be prepared to call when ordered, or on personal initiative in case of a serious incident. Think about giving the numbers to your neighbor so they too can respond to real or suspected incidents. Work out a series of overt and covert signals together.

-- Be sure all household members know the location of the telephone (and emergency numbers), fire equipment, fire escapes and other emergency exits, electrical service switches, weapons and emergency radio.

-- Ensure the family and servants are briefed on what to do in case of incident or emergency.

-- If awakened by a noise, it may mean someone has broken into the house. Turn on several lights and make as much noise as possible before checking. On discovering an intruder, immediately move the family to the prepared "safe room" before taking further action. Report the intrusion before investigating it, if possible.

-- If available, use a special purpose, hand held blinding bright light, while trying to find out their actions or criminal intent.

-- Select emergency exits to evacuate and escape.

-- In times of a high threat all household members should be prepared for an emergency evacuation. This emergency may include having suitcases packed. A reasonable sum of local currency should be kept on hand for such emergencies.

-- Make the house as fireproof as possible. Be sure fire extinguishers are available and in working order. They should periodically be checked and recharged as required.



28 MAR 1991

-- If guns are kept on the premises, follow the local laws governing their use. Weapons should be kept in a secure place in the home, particularly if stored while loaded. The weapon may or may not be stored loaded depending upon the threat. They must be kept away from the reach of children. Do not allow servants the chance to observe or tamper with such weapons. Those who might use and operate them must understand and practice safety rules.

-- Guns often serve better as a deterrent rather than as an active defense role. Use discretion and be sure of the target and need to use the weapon.

-- Keep MACE in the house and readily available. It may be preferred to using a gun, particularly in a low terrorist threat but high crime area, to lessen the chance of killing or wounding a burglar taken for a terrorist. Store the MACE beyond the reach of children.

-- Mail can be delivered to the office instead of the residence. If delivered at home, check all mail for suspicious features.

-- Do not accept unsolicited parcels. Have the carrier open them at a safe distance.

-- If strange boxes, packages, or other objects are discovered in a set of quarters or on the grounds, do not touch them, but immediately contact the appropriate security officer. If you think a parcel may contain a bomb, evacuate the area.

-- Consider putting in a high, perimeter fence as a defense against intruders. A tight hedge may also serve in this role. Tall trees or shrubs can serve as a screen to observe the house or grounds. Make sure gate fences are sturdy, in good repair and can be locked. There should be more than one gate throughout the grounds to provide alternative exits. Gates should be inspected periodically.

-- Keep the grounds to the quarters well lighted at night. Outside lighting is the cheapest and most effective deterrent to entry and cannot be overemphasized.

-- Shrubbery or other outside cover that is near gates could hide a terrorist and should be removed.

-- Be sure there are no concealed routes of approach to the house, such as a line of dense shrubbery.

-- Weapons and items that can be used as weapons, such as spears or knife displays, should not be in a place so intruders can take advantage and use them.



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

-- Lock doors to unused rooms. Lock as many doors as possible before going to bed. Double check all windows and doors to make sure they are locked. Keep skylights and roof hatches locked or barred at all times.

-- Safety chains should be placed on the inside of doors in the home. Door keys must be tightly controlled; carry them rather than hide them near the entrance.

-- Ensure positive identification is made before strangers or unexpected guests are admitted. A peephole or small windowlike opening in the door can identify a person before opening the door. Intercom or interview screen is also helpful.

-- Venetian blinds and shutters should be closed and locked at dusk; likely targets should not regularly stand in front of open windows. Consider adding bars over windows in high risk areas.

-- If bombs or missiles thrown through windows are a major threat, think about adding MYLAR, a thin and clear plastic sheet, to degrade their effect and to prevent casualties from flying glass. Heavy steel screens or security bars can also be added.

-- When on a trip, arrange to have the yard mowed and newspaper and mail collected. Leave a light on inside the house or use timers to randomly turn on lights. The confines of the house should be kept lighted when away.

-- When on a trip, tell the security officer so the house can be watched. Also, alert the local security forces and police.

-- Remember the telephone may be tapped so be discreet in disclosing information concerning travel, movement, schedules, or business matters.

-- When answering a telephone call, do not identify yourself. Answer "hello" first and make the other party tell you who is calling. In any case, don't give any unnecessary information.

-- Do not leave house keys on a car key ring when the car is being repaired or parked. Keep all keys under tight control and accountability.

-- Request police protection for large social events held in your quarters - particularly if likely targets are included on the guest list. Ensure the invited local nationals are reliable and not a security risk. Close control must be kept on the entrance of party guests.



28 MAR 1991

-- Do not attract attention to your residence by the manner in which you live. Do not display devices such as a US flag, name tag, or other signs that reveal your nationality. Consider having only a number, not a name, on the mailbox or door.

-- The appearance of alertness of the residents and staff serves as a deterrent. The practice of vigilance brings great psychological benefits at no cost.



28 MAR 1991

### VEHICULAR SECURITY

While preparing to depart or arrive in a vehicle, whether driving or being driven, you are particularly vulnerable to terrorists activity, assassination by bombing, gunfire, kidnapping, or harassment. The threat can be reduced by taking the following precautions:

-- Alertness is the first line of defense. Be observant at all times. Do not read or be in deep conversation or thought while in a vehicle. Your safety depends on your own awareness and good judgement.

-- Vary the route when going to and from work and if possible, the timing of trips. Extend this habit to other frequently visited places: clubs, restaurants, churches, schools, etc. Use different doors on entering and leaving. In establishing a variety of routes from home to office and back, do not fall into a repetitive pattern e.g., every third or fourth day you are repeating the same pattern. Primary targets should vary their position in the vehicle and also their dress.

-- Conceal planned departure and arrival times from those not directly concerned.

-- Know your vehicle, its capabilities and limitations.

-- Do not overload your car; it limits handling and degrades performance.

-- Park inside the fence or garage at home and not on the street. Garages should be locked.

-- At work, cars should be parked in a secure area, or guarded. If this is impossible, park in different areas daily.

-- Cars should always be locked when parked, or secured. Check carefully to see windows are fully closed. Never leave packages, purse, or clothing on car seats.

-- Before entering a car, even though it has been parked in a secure area, check it thoroughly: hood latch, gas tank cap, exhaust pipe, fender wells, any suspicious objects, or dangling and unexplained objects inside or underneath. If you suspect a bomb, do not tamper with it or attempt to remove it. Report your suspicions to the appropriate security officer who will take proper subsequent action. Keep away from the car and keep others away until the bomb squad arrives; have local police help if possible.

-- All vehicles should be equipped with hood and gas tank locks to hinder the quick attachment and concealment of bombs.

-- Gas tanks should be kept full and should be filled when the indicator shows 1/2 tankful.



28 MAR 1991

-- Gasoline should be provided through a government controlled facility or purchased on a random basis from local stations.

-- Fit cars with sonic warning device that sounds when hood is raised to prevent easy attachment of electric or other type of bombs, or bombs, or other tampering.

-- Equip cars with a loud siren or other audible device to activate in case of attack.

-- Vehicles commonly used by likely targets should be equipped with two-way mobile radios in the protective net. Consider also other clandestine warning devices available for attachment.

-- On very important person (VIP) vehicles, make it difficult for anyone to see the car is occupied. Curtains are an easy and cheap method.

-- If possible, use local rather than imported vehicles for official and personal use. Seek common color, model and make.

-- Use local license plates if allowed. Do not display anything that identifies the vehicle as belonging to an American citizen or other official.

-- If possible, rotate use of official vehicles so an individual cannot be identified with a particular car.

-- If armed guards are used for protecting selected individuals, generally they will ride in the front seat which facilitates their action.

-- If VIP vehicles have an organization escort, they will follow and not lead the VIP auto. If a host country escort is provided, particularly by police, they should go before the vehicle to give easy passage through traffic and lights.

-- If chauffeurs are used, ensure they have been cleared by local security forces. Repetitive checks should be made. Never tell drivers where you are going until ready to depart.

-- Chauffeurs must be trained in protective and defensive driving techniques. Rehearsals are appropriate. Retraining is also important. Chauffeurs must be trained until they can act instinctively.

-- When chauffeurs are employed, you decide the route to be used, where to stop or park and when you will depart and arrive. Give as little information as possible.



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

-- Be alert to possible surveillance at all times. Get in the habit of observing the traffic around you and be alert to any suspicious vehicle or vehicles behind you. Note any vehicle parked near intersections occupied by several persons. Passengers in your vehicle should share this task.

-- While driving, keep windows rolled up to within two inches from the top and lock all doors.

-- Stay near the middle of the road. This makes it difficult for terrorists to approach the car on the driver's side, their preferred direction of attack.

-- Be alert for trucks or other vehicles parked along the route when there are several persons in them; if one or more are observed, give them a wide berth when passing and drive at a high speed.

-- When driving, be sure a good distance is kept between you and the vehicle in front

-- particularly if it is a truck. This will allow you to avoid or pass the vehicle without being blocked.

-- Watch for suspicious persons following by vehicle or motorcycle. If one is observed, attempt to get the license number. If possible, try to lose it, drive to a preselected or observed "safe haven" such as a police station, pull into a public place, do not permit your vehicle to be closed in between cars.

-- Report the incident through channels to the local security forces for possible follow up.

-- Try to form a car pool of several persons riding together and if possible, form a convoy to travel between home and work.

-- If you must go out late at night, or must visit remote or strange areas, travel in pairs or groups and make sure someone knows your itinerary and destination. Always travel in at least twos at all times even in "safe haven" places.

-- Avoid remote and high risk areas at all times.

-- Avoid any observed civil disturbances - even if you must change direction or route drastically.

-- Avoid routes that have obstructions, such as construction, that could inhibit defensive driving techniques and could slow or halt your vehicle.

-- Avoid routes, particularly isolated ones, that offer terrorists opportunity for ambush or kidnapping attempts.



28 MAR 1991

- Avoid traveling at late hours.
- Determine and memorize the location of "safe havens" such as police or other security force posts along frequently used routes, or near often visited locations.
- Public transportation, when used with security in mind, may in some instances be preferable.
- If public transportation is used, do not use the same bus stop or taxi stand; vary time of departure and arrival. Buses are preferred to taxis.
- When using a taxi, know your route and do not let the driver deviate from it without obvious and known cause.
- Do not take the first available taxi. Do not set a pattern by taking the first, second, or third, etc.
- Do not request a taxi by telephone.
- Do not pick up hitchhikers.
- Keep the vehicle under control, but be sure to keep a normal speed in the flow of traffic - slow speed aids the attackers; excessive speed invites a crash incident.
- Ensure you and all passengers keep seat belts tightened at all times.
- Ensure you and your passenger(s) stay alert. Do not be distracted or your driver if being chauffeured; keep the noise level down. Keep the window rolled up on the driver's side and do not start any horseplay.
- Lock all doors of the vehicle until you arrive at your destination.
- Keep the motor in good tune. Ensure other systems such as lights, brakes, etc., are kept in excellent condition.
- Keep vision to the rear open. Keep packages off rear window and clothing off side windows. Lock all such items in trunk.



28 MAR 1991

PATTERN OF ATTACKS

Analysis of attacks by terrorists in kidnapping and assassination attempts against occupants in moving vehicles reveals consistent patterns. Understanding these tendencies and capitalizing on your knowledge of enemy vulnerabilities aids in counteracting the threat.

-- In nearly all cases the attack was conducted using two vehicles, one to impede or halt the target car, the other to box it in and maneuver the actual attackers close to the target. On occasion, more than two vehicles are used to halt the target car.

-- The attackers usually ride three or four people to a vehicle; a driver, a rider next to the driver and at least one person in the back seat. This frees two guns on one side and one gun on the other side.

-- "Pedestrians" may also take part in the attempt.

-- All known successful attacks have taken place from the driver's side of the target vehicle.

-- Attacks are usually conducted in an area having cross streets and by-ways to facilitate a quick get away.

-- Attacks seldom last for more than 15 seconds and if guns are used, only 10-15 rounds are normally fired by the attackers.

-- Witnesses are usually so confused they can offer no meaningful information to the police to aid in the investigation.

-- In most instances, a determined driver could break through the kidnapers vehicular blockades.

-- Questioning survivors of terrorist attacks against occupants of a vehicle revealed that:

(1) The attack was unexpected and completely by surprise. In retrospect they remembered warning signs that were not recognized or heeded before the attack.

(2) The target or the driver quickly became "boxed in" and lost freedom to maneuver.

(3) Instinctively, the driver attempted to evade the terrorist by veering away from their vehicles, to no avail. In fact, this is to the terrorists' advantage in that it gives them more room and you less room to maneuver to get a closer target for shooting.



28 MAR 1991

## PROTECTIVE DRIVING TECHNIQUES

Drive by thinking ahead; know what is happening two to three blocks ahead and to the rear of your vehicle. At any indication of terrorist action, initiate appropriate counterattack driving procedures explained below. Avoid, evade, crash then bypass, engage by fire, etc. For example, if you are obviously being followed by an unknown car with several occupants, take evasive action as a preventive measure:

-- Make a high-speed unsignaled turn (right or left) and circle the block.

-- If the followers persist, then drive to the nearest safe haven as quickly as possible.

-- Seek to put a bus, truck, or other slow moving vehicles between you and the suspect vehicle.

-- If it appears gun fire might start, have your unarmed passengers get down and stay down; crouch down as much as possible to minimize the observable target you offer.

-- If it appears you are going to be attacked from the rear, initiate your evasive action just as the pursuing car reaches your "blind spot" to the rear of the driver's side. Possible evasive actions include the following:

(1) Quick, unsignaled turns onto side streets.

(2) Sharp and repeated swerves to the right or left, forcing the attacker to take defensive action. With luck, this may force him into something.

(3) As an alternative, swerve left or right, then quickly stop, thus causing the attackers to unavoidably overrun your car and permitting you to quickly depart by the more direct, speedy route from the area.

-- Mentally prepare to receive bullet impacts.

-- In attacks using one or more vehicles in a moving or static cut off to halt or impede your movement, consider crashing the attacker:

(1) Ensure you can generate sufficient speed to make the strike effective.

(2) Seek a controlled crash -- strike where you select -- and keep control of your vehicle; jam your buttocks into the seat,



**PERSUPPACTSANDIEGOINST 5530.1B**

**28 MAR 1991**

keep both hands on steering wheel at 11 and 1 o'clock positions and spread knees and legs with outside leg braced against doory do not tense but assume a relaxed position.

(3) Seek to "clip" the halted or slowed vehicles that are impeding your route. Attempt to strike the vehicle on the extreme corners or at a wheel; seek a 45 degree angle.

(4) As an alternative, once you have decided to use the crash technique, quickly put on the brakes to gain maneuver/room and to change or interrupt the terrorist pattern, shift into low gear, pick a point to crash with maximum impact, speed through the block, then proceed to the nearest safe haven as quickly as possible.

-- In either crash technique, be sure not to attempt to merely "sideswipe" the opposing vehicle -- especially if the car is moving beside yours. This gives an opportunity to force you off the road, engage in gunfire at close range, or entangle your car. Seek to surprise the attacker with a quick maneuver or by braking to open a gap between cars, then, ram the car. The impact will make it difficult for the gunmen to fire, often immobilize the car and hopefully give you enough time to escape.

-- These techniques are not always successful. If they fail, you must decide whether to become a victim, or attempt to resist until help arrives.

28 MAR 1991

SECURITY RELATED EQUIPMENT

Security equipment is important in deterring or defeating attacks. Be sure all vehicles have the following general purpose items in usable condition:

- Inside rear view mirror.
- Outside rear view mirrors on each side.
- Seatbelts for each seat.
- Other special added equipment includes:
  - (1) Hood and gas tank locks
  - (2) Audible devices to warn when hood or trunk have been opened.
  - (3) Audible devices such as sirens or claxons to signal emergency
  - (4) Special communication equipment
  - (5) Ramming kits.
  - (6) Armoring kits in one of the several available degrees of protection.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



Appendix I:

Recall Bill



28 MAR 1991

APPENDIX I

PERSUPPACT SAN DIEGO

EMERGENCY CALL LIST

RECALL NUMBERS

FOR ESSENTIAL PERSONNEL

EACH PSD MAINTAINS INDIVIDUAL RECALL NUMBERS

FOR SAFETY SAKE KEEP THIS LIST UP TO DATE

FORWARD CHANGES TO CODE 11

PERSONAL DATA

THE RECALL LIST CONTAINS IDENTIFIABLE PERSONAL DATA WHICH IS TO BE SAFEGUARDED PURSUANT TO THE PRIVACY ACT OF 1974. THIS INFORMATION IS TO BE RELEASED ONLY TO AUTHORIZED PERSONNEL HAVING A NEED TO KNOW FOR OFFICIAL USES. WHEN NOT IN USE THE RECALL LIST IS TO BE STORED IN A LOCKED CABINET OR SECURED ROOM.



# PHYSICAL SECURITY AND LOSS PREVENTION PLAN



**Appendix J:**

PSD Specific  
Security Requirements



PERSUPPACTSANDIEGOINST 5530.1B

28 MAR 1991

APPENDIX J

PSD SPECIFIC SECURITY REQUIREMENTS

NOTE: Any PERSUPPACT, San Diego detachment who has any specific security requirements not met in this plan, will submit them for inclusion in this appendix.

