



DEPARTMENT OF THE NAVY

NAVAL AIR STATION OCEANA
VIRGINIA BEACH, VIRGINIA 23460-5120

Change 1 made 24 Sep 98
The changes have put in
with the originals.

NASOCEANAINST 5530.4C
15

31 OCT 1997

NAS OCEANA INSTRUCTION 5530.4C

Subj: PHYSICAL SECURITY PLAN

Ref: (a) OPNAVINST 5530.14B
(b) OPNAVINST 5510.1H
(c) OPNAVINST 5530.13B
(d) OPNAVINST 5500.4G
(e) OPNAVINST 5580.1
(f) OPNAVINST 11200.5C
(g) SECNAVINST 5500.29B
(h) OPNAVINST 5560.10B
(i) COMNAVIAIRLANTINST 5530.6
(j) COMNAVIAIRLANTINST 5530.11
(k) SECNAVINST 5530.5
(l) NASOCEANAINST 7321.1H
(m) NASOCEANAINST 5580
(n) NASOCEANAINST 5530.6
(o) NASOCEANAINST 5530.7
(p) NAVSUPINST 4440.115G
(q) NASOCEANAINST 11320.6A
(r) NASOCEANAINST 6280.2
(s) NASOCEANAINST 11345.1E
(t) NASOCEANAINST 8023.5
(u) NASOCEANAINST 3440.1
(v) NASOCEANAINST 11015.2
(w) OPNAVINST 3300.53

1. Purpose. This plan contains guidelines and procedures to be followed when implementing the Physical Security Program at Naval Air Station (NAS) Oceana. The contents discuss specific information to safeguard personnel, property and material through physical security and loss prevention measures.

2. Cancellation. NASOCEANAINST 5530.4B. Because of numerous revisions, paragraph markings have been omitted.

3. Responsibility. Maintaining effective security is the direct and immediate responsibility of all persons employed at NAS Oceana.

4. Action. Departments, tenant commands and other activities on board NAS Oceana shall be guided by this instruction and review

NASOCEANAINST 5530.4C

31 OCT 1997

the appropriate Navy Security Program guidance contained in references (a) through (w).



S. E. BENSON

Distribution:

NASOCEANAINST 5216.1Q

List I (Case A), II and III

13 1 OCT 1971

PHYSICAL SECURITY PLAN

TABLE OF CONTENTS

	Page	
Chapter 1	INTRODUCTION	
	0100 Purpose	1-1
	0101 Definitions	1-1
Chapter 2	CONTROL MEASURES	
	0200 General	2-1
	0201 Restricted Areas	2-1
	0202 Posting of Restricted Areas	2-3
	0203 Standards for Restricted Area Identification Passes	2-3
	0204 Restricted Area Personnel Identification and Control Procedures	2-3
	0205 Movement Control within Security Areas	2-4
	0206 Non-Restricted Areas	2-4
	0207 Non-Restricted Area Identification and Control Media	2-4
	0208 Personnel and Vehicle Inspections	2-5
Chapter 3	PROTECTIVE LIGHTING AND EMERGENCY GENERATORS	
	0300 General	3-1
	0301 Inspection and Maintenance	3-1
	0302 Power Failure	3-1
	0303 Emergency Generators	3-1
Chapter 4	PERSONNEL, VEHICLE ACCESS AND MATERIAL CONTROL	
	0400 General	4-1
	0401 Authorized Personnel Access	4-1
	0402 Authorized Vehicle Access and Identification	4-1
	0403 Commercial Vehicle Services	4-1
	0404 Vehicle Control	4-2
	0405 Material Control	4-2

31 OCT 1997

Chapter 5	INTRUSION DETECTION SYSTEMS (IDS)	
	0500 General	5-1
	0501 Responsibilities	5-1
	0502 Systems	5-1
	0503 Maintenance	5-2
	0504 Alarm Responses	5-2
	0505 IDS Locations	5-2
	0506 Emergency Power	5-2
Chapter 6	COMMUNICATIONS	
	0600 General	6-1
	0601 Communication Networks	6-1
	0602 Testing	6-2
	0603 Operations Security	6-2
Chapter 7	SECURITY DETACHMENT	
	0700 General	7-1
	0701 Organizational Billets	7-1
	0702 Posts and Routines	7-3
	0703 Crisis Management	7-3
Chapter 8	AUXILIARY SECURITY FORCE	
	0800 General	8-1
	0801 Composition	8-1
	0802 Mission	8-1
	0803 Weapons and Equipment	8-1
	0804 Coordinating Instructions	8-1
Chapter 9	SECURITY FORCE TRAINING	
	0900 General	9-1
	0901 Navy Security Training Requirement	9-1
	0902 Firearms Proficiency	9-2
	0903 Auxiliary Security Force (ASF) Training Requirements	9-2
Chapter 10	FLIGHTLINE AND SUPPORT FACILITY SECURITY	
	1000 General	10-1
	1001 Minimum Standards	10-1
	1002 Personnel Identification and Control Systems (PICS)	10-1
	1003 Flightline Security Requirements	10-2
	1004 Personnel Vehicle Control	10-2
	1005 Special Aircraft Security	10-3

31 OCT 1997

APPENDIX A	REFERENCES
APPENDIX B	MEMORANDUMS OF UNDERSTANDING
APPENDIX C	MAJOR ACCIDENT/DISASTER PROCEDURES
APPENDIX D	BARRICADED SUSPECT/HOSTAGE INCIDENT PLAN
APPENDIX E	BOMB THREATS
APPENDIX F	THREAT CONDITIONS
APPENDIX G	CIVIL DISTURBANCE
APPENDIX H	PHYSICAL SECURITY AND LOSS PREVENTION
APPENDIX I	CONTROL OF PHOTOGRAPHY
APPENDIX J	HUNTING INFORMATION
APPENDIX K	BUILDING SECURITY
APPENDIX L	CRISIS ACTION RESPONSE PLAN

31 OCT 1997

PHYSICAL SECURITY PLAN

CHAPTER 1

INTRODUCTION

0100. Purpose. Per references (a) through (w), this instruction establishes the following Security Program guidance and requirements for all departments, tenant commands and activities on board NAS Oceana:

- a. Evaluating, planning and implementing a Command Security Program.
- b. Physical security standards.
- c. Threat condition readiness.

0101. Definitions

a. Installations. All buildings, housing areas, facilities, land and roads within NAS Oceana property boundaries, including Naval Auxiliary Landing Field (NALF) Fentress, Navy Bombing Ranges Palmetta Point and Dare County, NC and Telephone Repeater Station, Cape May, NJ.

b. Physical Security. That part of security concerned with the physical measures and procedures designed to safeguard personnel, prevent unauthorized access to equipment, materials and documents against theft, damage, compromise and sabotage.

c. Areas of Security Interest. Those buildings, facilities or spaces whose contents contain property or personnel to which unimpeded access would pose a threat to the mission of this installation. Areas of security interest include arms, ammunition and explosives (AA&E) storage, bulk drug storage, classified information/equipment, property storage areas, automated data processing facilities and funds.

d. Physical Security Survey. A specific onsite examination and evaluation of Physical Security and Loss Prevention programs of an activity to determine vulnerabilities and compliance with the Navy Physical Security Program. The results of the survey are used as a management tool to improve the physical security of the activity.

e. Waiver. A temporary relief document (usually for a period of up to one year) from specific Navy Physical Security Program standards or requirements. The waiver includes compensatory security measures until these standards or requirements are met.

31 OCT 1991

f. Exception. A long term (36 month or longer) or permanent relief document from specific standards and requirements. The exemption includes compensatory security measures until these standards of requirements are met.

g. Restricted Areas. Three types of restricted areas are established in descending order of importance: Level Three, Level Two and Level One. Restricted areas shall be posted simply as "Restricted Area" so attention may not be drawn to the importance or criticality of an area. While restricted areas often pertain to the safeguarding of classified information, there are other valid reasons to establish restricted areas (e.g., mission sensitivity; protection of certain unclassified chemicals, precious metals or precious metal-bearing articles; conventional arms, ammunition and explosives; funds; drugs; nuclear material; sensitive or critical assets; articles having high likelihood of theft, etc.) to protect security interests.

(1) Level Three (Formerly Exclusion Area). The most secure type of restricted area. It may be within less secure types of restricted areas. It contains a security interest which if lost, stolen, compromised or sabotaged would cause grave damage to the command mission or national security. Access to Level Three restricted areas constitute, or is considered to constitute, actual access to the security interest or asset.

(2) Level Two (Formerly Limited Area). The second most secure type of restricted area. It may be inside a Level One area, but is never inside a Level Three area. It contains a security interest which if lost, stolen, compromised or sabotaged would cause serious damage to the command mission or national security. Uncontrolled or unescorted movement could permit access to the security interest.

(3) Level One (Formerly Controlled Area). The least secure type of restricted area. It contains a security interest which if lost, stolen, compromised or sabotaged would cause damage to the command mission or national security. It may serve as a buffer zone for Level Three and Two restricted areas, providing administrative control, safety and protection against sabotage, disruption or potentially threatening acts. Uncontrolled movement may or may not permit access to a security interest or asset.

PHYSICAL SECURITY PLAN

CHAPTER 2

CONTROL MEASURES

0200. General. The purpose of this chapter is to identify all controlled areas within NAS Oceana. The installation is a non-restricted area with various critical facilities and buildings designated restricted areas. All persons are forbidden to enter established restricted areas unless authorized.

0201. Restricted Areas

a. Departments, tenant commands and activities will establish and maintain minimum security measures per reference (a). The following areas are designated restricted areas:

<u>COMMAND</u>	<u>RESTRICTED AREA</u>	<u>LEVEL</u>
NASO Administration	Bldg 232 CMS Vault	3
NASO AIMD	Bldg 513 Avionics	2
NASO AIMD	Bldg 513-B Acetylene Storage	2
NASO AIMD	Bldg 513-C Oxygen/Argon Storage	2
NASO AIMD	Bldg 513-E Hazardous Waste Facility	2
NASO Air Operations	Flight Line/Aprons & Runways	2
NASO Air Operations	Bldg 3000 Radio Receiving	2
NASO Air Operations	Bldg 3001 Emergency Generator	2
NASO Air Operations	Bldg 3002 TACAN	2
NASO Air Operations	Bldg 3003 25KV Generator	2
NASO Air Operations	Bldg 3005 Antenna Platform	2
NASO Air Operations	Bldg 3015 Long Range Radar	2
NASO Air Operations	Bldg 3016 Radar	2
NASO Air Operations	Bldg 3017 Precision Approach Radar	2
NASO Air Operations	Bldg 3026 ACLS Trailer	2
NASO Air Operations	Bldg 3050 North Pad Facility	2
NASO Air Operations	Bldg 100 Air Traffic Control and	1
COMFITWINGLANT	Bldg 210 Intelligence Center	2
	Bldg 210 Room 107 & 116	3
COMFITWINGLANT	Bldg 150 Flight Simulators	2
	(1 st Floor)	
	Vault Room 118	2
	Simulator Room 137	2
	Simulator Room 128	2
COMFITWINGLANT	Bldg 150	
	(2 nd Floor)	
	Computer Room 211	2
	Computer Room 217	2
	IOS Room 212	2
	IOS Room 216	2

31 OCT 1997

<u>COMMAND</u>	<u>RESTRICTED AREA</u>	<u>LEVEL</u>
COMFITWINGLANT	Bldg. 140 Flight Simulator	2
COMFITWINGLANT	Bldg. 140 Vault 116 (E Wing)	2
COMFITWINGLANT	Bldg. 140 Vault 100 (D Wing)	2
COMFITWINGLANT	(1st Floor) Vault 101 (C Wing)	2
COMFITWINGLANT	(2nd Floor) (C Wing)	2
VACAPES	Bldg. 3030 Comm Center	3
VACAPES	Bldg. 3030 CMS Vault	3
VACAPES	Bldg. 3030 Control Floor	1
COMFITWINGLANT	Bldg. 140 Computer Rooms	3
	E-110/111, IOS E-205, and simulator E-114	
COMFITWINGLANT	Bldg. 240 Flight Simulator	2
COMFITWINGLANT	Bldg. 240 Compute, IOS and Simulator E-118/120, Maintenance Room E-119	2
COMMISSARY	Bldg. 290 Cashier Cage	1
NASO MWR	Bldg. 531 Cashier Cage	1
NAVAL WARFARE	Bldg. 310 Tactical Aircrew	1
ASSESSMENT CENTER	Combat Training (TACTS), Rooms 125-132	2
NAVY EXCHANGE	Bldg. 310 Room 124-Vault	3
NCIS	Bldg. 292 Cash Office	1
PSD	Bldg. 320 NW Wing Offices	2
SECURITY DETACHMENT	Bldg. 326 Disbursing-Room 115	1
SECURITY DETACHMENT	Bldg. 320 Armory (NE Wing)	2
	Dispatch Room	
NASO SUPPLY	Bldg. 720 Warehouse	1
NASO SUPPLY	Bldg. 722 Gen. Ready Issue	1
NASO SUPPLY	Bldg. 731 Storage Shed	1
NASO SUPPLY	Bldg. 823 HAZMAT Warehouse	1
NASO SUPPLY	Bldg. 720 Classified Material Cage	2
NASO SUPPLY	Bldg. 01 Fuel Pumping Station	2
NASO SUPPLY	Bldg. 608 Liquid Oxygen	2
NASO SUPPLY	Bldg. 608-A Liquid Oxygen Tank	2
NASO SUPPLY	Bldg. 608-B Liquid Oxygen Tank	2
NASO SUPPLY	Bldg. 608-C Liquid Oxygen Tank	2
NASO SUPPLY	Bldg. 608-D Nitrogen Tank	2
NASO SUPPLY	Fuel Storage Compound	2
NASO SUPPLY	Bldg. 121 Elevated Water Tank	1
NASO SUPPLY	Bldg. 602 Elevated Water Tank	1
NASO SUPPLY	Bldg. 1020 Water Treatment Plant	1
NASO SUPPLY	Bldg. 1021 Water Storage Tank	1
NASO SUPPLY	Bldg. 1022 Water Cutoff Pit	1
NASO WEAPONS	Bldg. 900 Ordnance Pad Facility	2
NASO WEAPONS	Bldg. 900-A Ready Service Magazine	2
NASO WEAPONS	Bldg. 900-B Ready Service Magazine	2
NASO WEAPONS	Ready Service Magazines 2500 - 2519	2

31 OCT 1997

0202. Posting of Restricted Areas. Restricted areas will be posted with a "Restricted Area" sign at all points of ingress (including buildings) per reference (a).

0203. Standards for Restricted Area Identification Passes

a. Permanent and temporary passes shall contain the appropriate information items per reference (a).

b. Permanent composition includes heat seal adhesion of the complete card to prevent photographic and information tampering. Passes shall be serialized and controlled.

c. Temporary passes shall include at a minimum a serialized clip-on badge recognizing the individuals as visitors under escort. Visitor pass identifying information shall be clearly legible to security personnel at a distance of one meter under normal lighting conditions.

0204. Restricted Area Personnel Identification and Control Procedures

a. The following guidelines shall be implemented for positive identification and control of military and Department of Defense civilian personnel entering restricted areas:

(1) Authorities to control entry.

(2) Identify media for personnel requesting entry.

(3) Record system to document time of entry and departure of personnel and visitors at all times.

(4) Access denial procedures/standards.

(5) Pass accountability system.

b. Visitors. Personnel requiring infrequent access to security areas and do not possess a permanent restricted area pass. The following guidelines shall be followed for the control of visitors:

(1) A visitor's pass shall be issued.

(2) One escort shall be provided by the organization visited for all restricted areas.

(3) A record system shall be maintained listing appropriate visitor and pass information, location visited and purpose.

31 OCT 1997

c. Contract Employees. Employees performing work in restricted areas shall be provided temporary access passes.

(1) Contract work located in restricted areas requiring employee access over a long period of time shall require local personnel security clearances.

(2) Small numbers of employee access over short periods of time shall require escorts if contractor personnel do not have the necessary security clearance authorization.

0205. Movement Control Within Security Areas. Personnel in restricted areas without authorized identification media or escorts are considered to be trespassers. They shall be detained and released to Security Force personnel for further disposition.

0206. Non-Restricted Areas. A non-restricted area is a limited or uncontrolled area. Such areas may be fenced or opened to the uncontrolled movement of the general public. Non-restricted areas shall not be located inside restricted areas. The following non-restricted areas are limited to residents and their guests:

a. Bachelor Officer Quarters (BOQ).

b. Bachelor Enlisted Quarters (BEQ).

c. All Quarters in Wadsworth, Trailer Park and the married officer's housing areas.

0207. Non-Restricted Area Identification and Control Media

a. Personnel Identification

(1) Military (Active). Armed Forces Identification Card, green in color (DD Form 2N).

(2) Military (Retired). Armed Forces Identification Card, gray or blue in color (DD Form 2).

(3) Military (Reserve). Armed Forces Identification Card, pink in color (DD Form 1172).

(4) Dependent. Armed Forces Identification Card, yellow or white in color (DD Form 1173).

(5) Civil Service. Armed Forces Identification Card, white in color (DD Form SF55).

(6) Contractors. Local NAS Oceana Identification Card (NASO Form 5530/2).

31 OCT 1997

b. Vehicle Decals

(1) Officer - NAS Oceana decal, blue in color, with date bars and DD Form 2220/11-79 DoD decal.

(2) Enlisted - NAS Oceana decal, red in color, with date bars and DD Form 2220/11-79 DOD decal.

(3) Civil Service -NAS Oceana decal, green in color, with date bars and DD Form 2220/11-79 DOD decal.

(4) Contractor - NAS Oceana decal (white in color) with date bars and DD Form 2220/11-79 DOD decal.

(5) Temporary Pass - Local Oceana white card with vehicle owner information and expiration date; valid for 90 days.

(6) Visitor Pass - Various colors; valid from 0600 to 2400 hours the same date.

0208. Personnel and Vehicle Inspections. This security measure is implemented to reduce the unauthorized removal of government property and deter the introduction of contraband. Administrative inspections will be conducted on a random basis as directed by the NAS Oceana Commanding Officer.

31 OCT 1997

PHYSICAL SECURITY PLAN

CHAPTER 3

PROTECTIVE LIGHTING AND EMERGENCY GENERATORS

0300. General. Protective lighting is a tool used to assist in maintaining a level of security commensurate with the level maintained during daylight hours. It enhances the local security posture during darkness to ensure a safe operating environment.

0301. Inspection and Maintenance. The Base Civil Engineering Department manages all installation maintenance and testing of protective lighting and emergency generators. Command Duty Officers, supervisors and Security Force personnel shall report inoperative protective lighting to the Base Civil Engineering Department for repair.

0302. Power Failure. In the event of a power failure, the Public Works Department shall take appropriate actions to restore power. When required, portable lighting systems shall be used to illuminate installation access areas and mission critical areas for operation.

0303. Emergency Generators. Installed at vital and significant sites. They shall be kept in a mission ready status. The following installation sites have emergency generators:

<u>BUILDING #</u>	<u>FACILITY</u>	<u>GENERATOR</u>
100	Main Tower	220KW
3001	Receiver Site	30KW
3015	Main Radar	125KW
Midfield	PAR	30KW
Midfield	ACLS	125KW
3003	TACAN	60KW
1201	Field Lighting Vlt	200KW
Runway 23	Light Vault	4KW
20	Fentress	200KW
3031	VACAPES	460KW
E105	Fuel Day Tanks	60KW
520	Galley	60KW
Hangar 500	FITWING	30KW
320	Security Detachment	10KW
220	Fire Station	100KW
E108	Tower Field Lighting	150KW
230	Administration	50KW
285	Clinic	200KW
601	Boiler Plant	275KW
SD 600	Main Sewage Station	150KW
SD 3001	Wherry Sewage Station	60KW
SD 6042	Wadsworth Sewage Station	150KW

31 OCT 1997

PHYSICAL SECURITY PLAN

CHAPTER 4

PERSONNEL, VEHICLE ACCESS AND MATERIAL CONTROL

0400. General. Per references (a), (f) and (h), this chapter discusses policy and procedure for access identification and movement control of personnel, vehicles and material on board NAS Oceana.

0401. Authorized Personnel Access

- a. Active duty and retired military personnel, dependents and DoD civilians.
- b. Civilian personnel employed by tenant activities.
- c. Contractor personnel with active contracts.
- d. Individuals with authorized base privileges.
- e. Reservists.
- f. Guests, vendors and other visitors authorized access after receiving a pass.

0402. Authorized Vehicle Access and Identification

- a. Motor vehicles operating on the installation must display a current DoD Decal or other Hampton Roads Navy installation media. Government owned or leased vehicles and contractor equipment at job sites are exempt from this requirement.
- b. Persons operating motor and recreational vehicles on the installation shall comply with the vehicle and traffic regulations per reference (h).
- c. Off-road vehicle use on government property is strictly prohibited.

0403. Commercial Vehicle Services

a. Taxi Service. Taxi services are authorized for embark and debark fares only. Taxis are not authorized to solicit transportation services on the installation and must meet the following commercial vehicle requirements:

- (1) Be metered.
- (2) Equipped with an exterior roof mounted light.

31 OCT 1997

(3) Operating permit issued by the City of Virginia Beach.

0404. Vehicle Control. The control of vehicle movement is contained in references (a) and (f).

a. Parking is not permitted in level two and three restricted areas unless a physical security waiver or exception has been approved per reference (a).

b. General Parking Restrictions

(1) Areas marked by a sign or painted curb.

(2) Within 15 feet of a fire hydrant.

(3) Grass and unpaved areas unless specifically designated for parking by authorized signs.

(4) Where the movement of vehicle and pedestrian traffic would be impeded or blocked (i.e., streets, jogging paths, sidewalks, etc.).

(5) Fire and security station areas.

0405. Material Control. Every precaution shall be exercised to ensure the security and accountability of government material is maintained. Additional security measures shall be used to enhance internal security and loss prevention.

a. Supplies. Special controls for the delivery of supplies and shipments to restricted areas are contained in reference (a).

b. AA&E. AA&E shall be handled per reference (t). Shipment of weapons entering NAS Oceana shall be escorted by the Security Detachment to the Weapons compound safe haven and refuge holding areas per references (m) and (t).

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

(1) Handling. Hazardous materials shall be handled per references (r) and (s).

31 OCT 1997

PHYSICAL SECURITY PLAN

CHAPTER 5

INTRUSION DETECTION SYSTEMS

0500. General. Intrusion Detection Systems (IDS) consist of sensors and energy sources capable of detecting entry or attempted entry into an area. The NAS Oceana IDS Program is a proprietary type per reference (a), supported by 24 hour monitoring and armed Security Detachment response.

0501. Responsibilities

a. The Security Officer shall ensure all alarms are monitored and physically examined at least once every six hours and provide armed response to alarm activations.

b. Commanding Officers of user activities are responsible for the proper installation of local alarms, monthly systems testing, alarm operation schedules and maintenance.

c. Activities with IDS alarm systems are responsible for funding of and maintaining contacts for the repair and maintenance of their systems.

0502. Systems. The following NAS Oceana systems guidance is provided:

a. The Central Control Panel Monitoring Station provides visual and audible alarm capabilities located at the Security Detachment.

b. Intrusion Alarm Systems will provide an alarm signal at the monitoring station when the system is in the secure and access modes. All alarm equipment is activated in the secure mode; line supervision and anti-tamper switches are activated in the access mode.

c. Key switches used to activate and deactivate alarms shall not be installed in unsecured areas.

d. Alarm operation schedules shall be provided for each alarm system. Schedules shall be coordinated with the Security Detachment.

31 OCT 1997

e. Activities protecting restricted areas shall use "word recognition codes," coordinated with the Security Detachment, for scheduled activation and deactivation of alarms. Word codes shall be used via telephone to the Security Detachment dispatcher. Additionally, a duress code system shall be included in these procedures.

0503. Maintenance. Emergency maintenance shall be conducted as soon as possible. Maintenance technicians shall test and inspect all systems quarterly, including the testing of backup and emergency power sources, and maintain records of systems tests and maintenance.

0504. Alarm Responses. The Security Detachment shall respond appropriately to all activated alarms. Alarm activations during normal working hours will require coordination with building supervisors to determine the alarm status. After normal working hours, building supervisors shall be recalled to open and examine their building with Security Force personnel.

0505. IDS Locations

<u>BLDG. #</u>	<u>COMMAND/ACTIVITY</u>
137	Strike Weapons and Tactics School Atlantic
140	Fighter Wing Atlantic
150	Fighter Wing Atlantic
210	Fighter Wing Atlantic
240	Fighter Wing Atlantic
285	Branch Medical Clinic
290	Commissary
292	Navy Exchange
294	Navy Exchange
295	Navy Exchange
310	Tactical Aircrew Combat Training System
320	Naval Criminal Investigative Service
326	Personnel Support Detachment
430	Morale, Welfare and Recreation
480	Morale, Welfare and Recreation
528	Navy Federal Credit Union
531	Morale, Welfare and Recreation
532	Nationsbank
541	Navy Exchange
542	Navy Exchange
SR-6	Morale, Welfare and Recreation
TS-1	Morale, Welfare and Recreation

0506. Emergency Power. An emergency back-up generator or battery operated system shall provide uninterrupted power to all IDS when normal power is lost or interrupted.

31 OCT 1997

PHYSICAL SECURITY PLAN

CHAPTER 6

COMMUNICATIONS

0600. General. Internal and external telephone networks are the primary communication systems used by NAS Oceana and tenants. UHF-FM radio communication networks are used by various departments for routine and emergency operations.

0601. Communication Networks

a. Internal. The internal communication networks are the telephone and VHF-FM radio communication systems.

(1) Telephone. The base wide non-secure emergency internal telephone numbers are:

- (a) Security - 3-9111
- (b) Fire - 3-9111
- (c) Medical - 3-2221

(2) VHF-FM Radio. The network is comprised of a base station and vehicle mounted or hand-carried transceivers. The primary NAS Oceana VHF nets are:

<u>Net</u>	<u>Frequency</u>	<u>Users</u>	<u>Mode</u>
Security Detachment	143.725MHz (TX) 140.225MHz (TX)	Security Force Fire Department Base MAA	Secure and Non- Secure
Disaster Preparedness	140.150MHz	Disaster Preparedness Organization	Non- Secure
Base Civil Engineer	138.550MHz	BCE Tenant Commands	Non- Secure
Air Operations	141.000MHz	Air Ops	Non- Secure

b. External. The external communication networks are the non-secure DSN system, non-secure commercial system and STU III secure voice system.

NASOCEANAINST 5530.4C

31 OCT 1991

0602. Testing. Security and fire response emergency communication circuits and equipment shall be tested daily and results recorded by the Security Detachment Dispatcher. Additionally, maintenance shall be conducted monthly and discrepancies corrected as soon as possible.

0603. Operations Security. Radio and telephone communications over the networks are generally unsecured. Information of a classified nature shall not be discussed over unsecured telephone or radio networks.

31 OCT 1991

PHYSICAL SECURITY PLAN

CHAPTER 7

SECURITY DETACHMENT

0700. General. Per reference (a), the NAS Oceana Security Detachment administers to, and implements Navy Security programs within its jurisdiction.

0701. Organization and Billets

a. Administration Division. Responsible for the administrative management of the detachment.

(1) Security Officer. Administers to the command Physical Security, Law Enforcement, Anti-terrorism and Loss Prevention programs. Manages installation Security Forces and related assets.

(2) Assistant Security Officer. Plans, manages and implements command Physical Security, Law Enforcement, Anti-terrorism and Loss Prevention programs.

(3) Physical Security Officer. Assists in determining physical security requirements, conducts surveys and reviews Physical Security Plans. Manages Security Detachment IDS, key control and ADP programs.

(4) Administrative Officer. Plans and manages the Administrative Division. Trains administrative personnel and supervises all administrative functions.

(5) Pass Office Clerk. Manages the issue and accountability of installation access media.

(6) Traffic Court Judge. Processes minor installation traffic code violations and manages related administrative accountability.

(7) Administrative Assistants. Manages correspondence, associated files and supply processes.

(8) Loss Prevention Officer. Plans and manages all Crime Prevention programs. Conducts crime prevention lectures, maintains associated statistical data and manages the Missing-Lost-Stolen-Recovered Government Property Program.

31 OCT 1997

b. Investigation Division. Responsible for investigating all violations of the Uniform Code of Military Justice waived under the jurisdiction of the Naval Criminal Investigative Service (NCIS). Maintains effective coordination with NCIS, local and other federal authorities.

(1) Investigations Officer. Plans and manages the Investigative Division. Trains command Investigators and supervises all investigative functions.

(2) Command Investigator. Conducts investigations and safeguards evidence.

(3) Warrants/Summons Officer. Installation coordinator with civil authorities to issue city and state warrants and summons.

c. Operations Division. Responsible for field security operations, law enforcement and other field support management.

(1) Operations Officer. Plans and manages the Operations Division. Implements policy and procedures for field security operations and supervises all operational security functions.

(2) Watch Commander. Supervises a patrol section, implementing field security functions.

(3) Dispatcher. Manages communication networks, Intrusion Detection Systems, coordinates response to emergencies (fires, medical, security) and maintains associated logs and desk journals.

(4) Patrolman. Performs field security and law enforcement duties.

(5) Kennel Master/Military Working Dog Handler. Plans and manages the Military Working Dog (MWD) Program. Performs routine patrol functions and narcotic detection services with personally trained MWD.

(6) Training Officer. Plans, manages and implements Navy Security Force training programs for permanent, auxiliary and reserve Security Force personnel.

(7) Auxiliary Security Force Coordinator. Plans and manages the installation Auxiliary Security Force Program.

NASOCEANAINST 5530.4C
31 OCT 1997

0702. Posts and Routines. All fixed and mobile post orders are listed in reference (m). Divisional duties and routines are implemented in support of the Command Security Plan.

0703. Crisis Management. The management of response procedures are contained herein and in references (m) and (u).

31 OCT 1997

PHYSICAL SECURITY PLAN

CHAPTER 8

AUXILIARY SECURITY FORCE

0800. General. The Auxiliary Security Force (ASF) is a supplemental security organization, trained and activated to augment the permanent Security Force when directed by the Commanding Officer.

0801. Composition. ASF manpower is derived from NAS Oceana departments and non-deployable military tenant commands on board NAS Oceana. Force quotas are determined by post requirements and the activities' enlisted population (E-6 and below).

0802. Mission. The ASF is activated during security exercises, increased threat conditions, man-made and natural disasters or other evolutions as directed by the Commanding Officer.

0803. Weapons and Equipment. ASF members shall be qualified with the .9MM pistol, 12 gauge shotgun and other weapons as required per reference (a). All security equipment required for duty shall be issued by the Security Detachment. The authorized uniform for this duty is camouflage utilities.

0804. Coordinating Instructions. Specific organization and training guidance is provided in references (a), (m) and (o).

31 OCT 1997

PHYSICAL SECURITY PLAN

CHAPTER 9

SECURITY FORCE TRAINING

0900. General. This chapter defines the NAS Oceana Physical Security and Law Enforcement training requirements per reference (a).

0901. Navy Security Training Requirements

a. Phase I Training. Military personnel who perform full time physical security and law enforcement duty must successfully complete the Navy Security Guard school or Master-at-Arms "A" school.

b. Phase II. This in-service security training course is conducted by the Security Detachment.

(1) Initial. Personnel who report for Security Duty receive a 120 hour course of instruction per reference (a).

(2) Annual. A minimum of 40 hours of refresher security training is conducted annually per reference (a). Permanent Security Force personnel receive a minimum of four hours per month of field and classroom training to include weapons qualification and proficiency.

c. General Military Training (GMT). GMT is a monthly command sponsored training requirement. It provides information and instruction about other Navy programs and requirements (i.e., safety, physical fitness, operation security, environmental, career, etc.).

d. Guardmount Training. Conducted 20 to 30 minutes prior to each patrol section rotation of the Operations Division. This training reviews standard operating procedures, safety and local policies and directives.

e. Job Qualification Requirements (JOR). This is a local Field Qualification Manual issued to Security Force personnel during the initial Phase II In-service training. It standardizes special technical and field service requirements for operational billets in the Security Detachment.

31 OCT 1997

0902. Firearms Proficiency. Security Force personnel shall maintain weapons qualification with the .9MM pistol, 12 gauge shotgun, M-14 rifle and M-60 machine gun (as required) per reference (a). The 9MM pistol is carried by all security force personnel in a duty status and the following courses of fire are to be successfully completed prior to receiving authorization for the carrying of this weapon:

a. Naval Qualification Course. Fired three consecutive times annually for qualification, unless qualification standards are met during the first or second course of fire.

b. Night Fire Course. Fired two consecutive times annually for qualification, unless qualification standards are met during the first course of fire.

c. Practical Weapons Course. Fired two consecutive times semi-annually, unless qualification standards are met during the first course of fire.

0903. Auxiliary Security Force (ASF) Training Requirements

a. Initial Phase I Training. ASF personnel shall successfully complete a 120 hour basic training course conducted by the NAS Oceana Security Detachment. The minimum training requirements are contained in references (a) and (o).

b. Phase II Training. ASF personnel shall attend two days of field and classroom training per month and integrated into daily security force operations for drill and on-the-job training.

PHYSICAL SECURITY PLAN

CHAPTER 10

FLIGHTLINE AND SUPPORT FACILITY SECURITY

1000. General. This chapter establishes uniform flightline security standards and procedures per reference (a).

1001. Minimum Standards

a. Restricted Area. The flightline property, within the man-made natural barriers surrounding the runways to include all buildings and structures, is designated a Level Two Restricted Area.

b. Access Points. All ingress and egress areas shall be controlled. Tenants managing flightline gates shall:

(1) Lock all gates when not in use.

(2) Control locks and keys to flightline gates per reference (a) and this instruction.

(3) Implement a uniform flightline Personnel Identification and Control System per reference (a) and this instruction. Only personnel with appropriate flightline identification shall be authorized access.

1002. Personnel Identification and Control System (PICS). This is a mandatory security measure for all Level Two Restricted Areas per reference (a). Personnel requiring flightline access shall have a serialized NAS Oceana flightline decal affixed to their official military or civilian identification card or issued an appropriate temporary pass for flightline access. PICS flightline decals are as follows:

a. 3/4 inch diameter (circular in shape) with blue background.

b. Six digit alpha numeric serial number with black numbers.

c. The international Civil Aviation Organization code "NTU," with black letters.

31 OCT 1991

1003. Flightline Sentry Requirements. Reference (a) sets specific guidance for sentry personnel. The minimum training requirements for NAS Oceana flightline sentry personnel are:

a. Formal instruction on installation flightline security sentry procedures.

b. Completion of flightline sentry Job Qualification Requirements.

1004. Personnel/Vehicle Control. Personnel and vehicle access to the flightline shall be limited to official business only and strictly controlled.

a. Personnel requiring flightline access shall be issued local PICS decals or visitor passes.

b. All primary vehicle and pedestrian access areas into the installation shall be identified with signs as required by reference (a), indicating all personnel are subject to search at anytime while within the flightline area. Random inspections by Security Force personnel may be conducted as directed.

c. There are sixteen authorized access areas on the flightline:

- (1) Post #4 - D Avenue and Hangar #122
- (2) Post #5 - B Avenue and Hangar #111
- (3) Post #6 - 1st Street and Hangar #23
- (4) Access Gate (not numbered) - Northeast corner of Hangar 200; secured
- (5) Post #7 - Princess Anne Road and Hangar 200
- (6) Post #8 - Hangar #404 (East Side)
- (7) Post #9 - 4th Street and Hangar #500
- (8) Post #10 - Hangar #500 (East Side)
- (9) Post #11A - 5th Street and Hangar #500 (South Side)
- (10) Post #12 - London Bridge Road and Weapons Gate
- (11) Post #13 - VACAPES and Oceana Boulevard

31 OCT 1991

(12) Post #13B - Access Gate off road Old Colonial Road behind back gate of FACSFAC VACAPES

(13) Post #14 - Oceana Boulevard and Bells Road

(14) Post #15 - London Bridge Road (Southwest Side of Base)

(15) Post #24 - Access gate off Potters Road to Skeet Range

(16) Post #27 - Access gate off Potters Road to radar and receiver site

(17) Post #28 - Access gate off London Bridge Road to Fuels compound

d. Reference (m) requires personnel accessing and operating vehicles on runways and taxi areas of the airfield to possess a valid airfield operator's permit or be escorted in a vehicle by an individual with a permit. Additionally, vehicles operating in this proximity shall possess rotating, illuminated beacon devices (yellow for utility vehicles; red for emergency vehicles) or a checkered flag (3ft square) with international orange and white colors prominently displayed and two way radio communications with tower. Radios may be checked out at the NAS Oceana Air Operation Department.

1005. Special Aircraft Security. Special aircraft transiting NAS Oceana may require armed security support. Special security measures will normally be implemented by military or civilian security organizations responsible for the aircraft. Installation Security Force personnel may be required to implement special aircraft security measures.

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX A

REFERENCES

- (a) OPNAVINST 5530.14B Physical Security and Loss Prevention Manual
- (b) OPNAVINST 5510.1H DoN Information and Personnel Security Program Regulation
- (c) OPNAVINST 5530.13B DoN Physical Security Instruction for Conventional Arms, Ammunition and Explosives (AA&E)
- (d) OPNAVINST 5500.4G Reporting of Missing, Lost, Stolen or Recovered Government Property (MLSR)
- (e) OPNAVINST 5580.1 Law Enforcement Manual
- (f) OPNAVINST 11200.5C Motor Vehicle Traffic Supervisor (NOTAL)
- (g) SECNAVINST 5500.29B Use of Deadly Force and the Carrying of Firearms by Personnel of the Department of the Navy in Conjunction with Law Enforcement Protection
- (h) OPNAVINST 5560.10B Standard Procedures for Registration and Marking of Non-Government Motor Vehicles
- (i) COMNAVAIRLANTINST 5530.6 Physical Security Electronic Equipment (PSOAI)
- (j) COMNAVAIRLANTINST 5530.11 Security Lighting
- (k) SECNAVINST 5530.5 Security of Selected Sensitive, Inventory Items - Drugs, Drug Abuse and Precious Metals
- (l) NASOCEANAINST 7321.1H Management Procedures for Class 1, 2, 3 and 4 Plant Property
- (m) NASOCEANAINST 5580 Security Detachment Standard Operating Procedures (SOP) Manual

NASOCEANAINST 5530.4C

31 OCT 1997

(n) NASOCEANAINST 5530.6	Physical Security Plan, Naval Auxiliary Landing Field, Fentress
(o) NASOCEANAINST 5530.7	Auxiliary Security Force (ASF)
(p) NAVSUPINST 4440.115G	Physical Inventory Program
(q) NASOCEANAINST 11320.6A	Fire Prevention Regulation and Instruction Bill
(r) NASOCEANAINST 6280.2	Reporting and Clean-up of Hazardous Material Spills
(s) NASOCEANAINST 11345.1E	Hazardous Waste Disposal
(t) NASOCEANAINST 8023.5	Explosives Handling Personnel Qualification/Certified Training Program
(u) NASOCEANAINST 3440.1	Disaster Preparedness and Recovery Plan (DPRP)
(v) NASOCEANAINST 11015.2	Hunting and Trapping
(w) OPNAVINST 3300.53	Navy Combating Terrorism Program

PHYSICAL SECURITY PLAN

APPENDIX B

MEMORANDUMS OF UNDERSTANDING

1. The following Security Memorandums of Understanding are maintained at the NAS Oceana Comptroller Office:

a. Chief of Police, City of Virginia Beach, Municipal Center, Virginia Beach, VA 23456-9064, MOU# N60191-91084-066.

b. Chief of Police, P. O. Box 15225, Chesapeake, VA 23320, MOU# N60191-95093-055.

c. Palmetta Point, Tyrell County Sheriff, Columbia, NC 27925, MOU# N60191-89101-054.

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX C

MAJOR ACCIDENT AND DISASTER PROCEDURES

1. General. To provide direction for action involving major accidents or disasters.
2. Action. Specific actions and duties are set forth in reference (u) listed in Appendix A of this instruction.

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX D

BARRICADED SUSPECT/HOSTAGE INCIDENT PLAN

1. Purpose. To establish procedures and provide guidance for countering barricaded captor/hostage incidents in accordance with the requirements of reference (a).
2. Discussion. There are three operational considerations in a hostage situation:
 - a. Protection of life including the perpetrators.
 - b. Protection of government property.
 - c. Safeguarding classified material.
3. Actions. On notification of a hostage situation on board NAS Oceana, the following actions shall be implemented:
 - a. Commanding Officer. The Commanding Officer, Naval Air Station Oceana or his representative will exercise command and control during a barricaded captor or hostage incident at the Command Center (Building #232).
 - b. Security Detachment
 - (1) Security Officer. Act as On-Scene Commander until relieved by the Naval Criminal Investigative Service, maintain operational control of Security Forces and coordinate with local authorities for incident support.
 - (2) Security Detachment Operations Division Officer. Act as Tactical On-Scene Commander responsible for the employment and direction of all on-scene, responding security and local authorities support.
 - (3) Dispatcher. Notify the following:
 - (a) Security Detachment Staff
 - (b) NAS Oceana Quarterdeck and Command Duty Officer
 - (c) NCIS Duty Agent
 - (d) Branch Medical
 - (e) Fire Department

31 OCT 1997

(4) Patrolman. Establish an immediate perimeter surrounding the effected area, evacuate all non-essential personnel and contain the incident. Additionally, establish an outer perimeter to maintain a clear zone around the incident area.

c. Naval Criminal Investigative Service. The duty agent shall provide hostage negotiators and assist the Tactical On-scene Commander.

d. Branch Medical Clinic. Provide ambulance services.

e. Fire Department. Provide firefighting and paramedic services.

f. Command Duty Officer. Brief Commanding Officer on incident status and prepare operational message reports.

g. Base Civil Engineering Department. Provide appropriate building floor plans and blue prints.

h. Public Affairs Officer. Provide information for media release when required.

22 SEP 1998

PHYSICAL SECURITY PLAN

APPENDIX E

BOMB THREATS

1. Purpose. To establish procedures and provide guidance for bomb threats and suspected explosive devices (SED).
2. Discussion. The most frequent method of receiving a bomb threat is by telephone and any such report should be treated as a real threat.
3. Actions
 - a. The following procedures shall be followed by personnel receiving a bomb threat by telephone:
 - (1) After receiving the bomb threat, notify the Security Department (433-9111/3101) and the immediate chain of command.
 - (2) Ensure a Navy Telephonic Threat Complaint Form (OPNAV5527/8) is completed.
 - b. Security Department
 - (1) Establish a command control post at the scene. The Watch Commander shall be the Tactical On-scene Commander.
 - (2) Take necessary precautions for the safety of all personnel and establish a safety perimeter of approximately 300 feet (when possible) from the threatened area. Utilize Security personnel for perimeter, crowd and traffic control.
 - (3) Ensure all traffic is routed around the incident area with the exception of emergency and official vehicles.
 - (4) Maintain coordination with NAS Oceana Commanding Officer, Command Duty Officer and Commanding Officers of tenant commands to implement evacuation, search procedures and incident guidance.
 - (5) Notify NAS Oceana Quarterdeck of the incident and if necessary, medical; EOD; fire department and request assistance from COMNAVBASE for Explosive Detector MWD Team.
 - c. Fire Department
 - (1) Respond to scene with adequate personnel and equipment.

22 SEP 1998

(2) Do not use lights and sirens in the vicinity of the incident area and limit radio transmissions within the affected areas.

d. Medical Department. Respond to incident area with an ambulance and corpsmen when directed.

e. NAS Oceana Quarterdeck. Notify Commanding Officer, Executive Officer and Command Duty Officer.

f. Public Affairs Officer. Provide information for media release (when required).

g. Building Evacuation

(1) Evacuate building and area safely, using emergency egress routes per local standard operating procedures.

(2) Remove all personal items such as briefcases, bottles, lunch bags, etc., and secure radios and other electrical equipment from building.

(3) Interior and exterior windows and doors shall remain open to help dissipate potential explosive forces.

(4) All cabinets and drawers shall be left unlocked, except those securing classified materials.

(5) Secure building after evacuation to prevent reentry by unauthorized personnel.

(6) Allow vehicles in front of buildings to depart at exits determined by the Tactical On-Scene Commander.

(7) Evacuate and muster all remaining personnel in an area determined by the Tactical On-Scene Commander at least 300 feet away from the affected area.

(8) Allow personnel leaving the Commissary or NEX to exit the area with their privately owned vehicles.

h. Bomb Search Guidance. Searches are best conducted by two person teams that are familiar with the suspected spaces or buildings. There are various search methods which could be implemented, but the following method is recommended:

(1) Move to various areas within the space and stand quietly, with eyes closed and listen for unusual sounds (i.e., beeps, ticking). Frequently, a clock-work mechanism can be quickly detected without the use of special equipment or devices. Even if a clock-work mechanism is not found, the search team is now aware of the background noise level of the space itself.

22 SEP 1998

(2) Observe the space and determine how the area is to be divided for search procedures based on the number and type of objects in the space.

(3) Conduct the search pattern from the deck to the overhead. Begin the search procedures at the perimeter wall of the space and work towards the center.

(4) When a suspected device is found, notify the Tactical On-Scene Commander, mark the device's location and continue to search for other devices until the space is cleared. The device shall not be touched by anyone other than EOD.

(5) After the space has been searched, post a sign or marker to indicate a bomb search has been completed.

(6) Ensure all spaces are searched.

(7) If a detonation time is known, a 15-minute waiting period shall take place prior to space reentry.

i. Reentry Approval. Once evacuated from any building or area, personnel shall not be permitted reentry unless authorized by the host or tenant Commanding Officer or direct representative.

4. Special Incident Reports. The Command Duty Officer shall report bomb threat incidents by message and phone per reference (b). The activity receiving the bomb threat is responsible for submitting the Special Incident Report (SITREP/OPREP).

5. Bomb Threat Drills. An annual bomb threat drill is recommended to exercise evacuation plans and provide bomb search training.

22 SEP 1998

PHYSICAL SECURITY PLAN

APPENDIX F

THREAT CONDITIONS FOR COMBATING TERRORISM

1. Purpose. To define and establish Treat Condition Alert levels and actions to be taken in response.
2. Background. Previous instances of increased physical security levels necessitated the issuance of random, haphazard and ambiguous instructions which did little more than confuse those responsible for carrying out those instructions.
3. Definitions. This section provides definitions of those terms utilized in this appendix.
 - a. Anti-terrorism. Measures used to reduce vulnerability of DoD personnel, their dependents, facilities and equipment to terrorist acts.
 - b. Counter-terrorism. Measures taken in reaction to a terrorist incident.
 - c. Terrorism. Unlawful use or threatened use of force or violence against individuals or property, with intention of coercing or intimidating governments or societies, often for political or ideological purposes.
 - d. Terrorist THREATCON. Formal level of anti-terrorist readiness, directed by the Commander to upgrade physical security readiness to deter terrorist attack.
4. Assessment Factor Definitions. Assessment factors provide background for general guidelines in uniform implementation of alert conditions:
 - a. Capability. Applies when a terrorist group has the ability to carry out an operation against U.S. interests in areas of concern. This includes resources such as intelligence, mobility, personnel, etc.
 - b. Existence. Applies when a terrorist group is present in an area of concern. The group need not have posed a threat to U.S. or DoD interests in the past.
 - c. History. Applies when a group's history of terrorist acts and behavior reflect an anti-U.S. stand or includes previous attacks against U.S. interests.

22 SEP 1998

d. Targeting. Applies if there are known plans or confirmed intentions of a terrorist group to target U.S. or DoD interests. Targeting can be either specific or nonspecific. If targeting is not against a U.S. or DoD interest, this factor should not be considered.

e. Trends. Applies if the group has, over the past year, displayed significant terrorist activity that appears to be continuing or increasing. Activity need not have been violent (e.g., terrorist attack against U.S. or DoD interest could be rhetorical or threatening utterances or statements). This factor could be flexible depending on the length of the group's activity cycle.

5. THREATCONs and Measures To Be Taken To Limit Their Success

a. THREATCON ALPA. A general warning of possible terrorist activity, the nature and extent of which are unpredictable, where circumstances do not justify full implementation of the measures contained in 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 of strangers, particularly those carrying suitcases or other containers; be alert for unidentified vehicles on, or in the vicinity of, Naval installations and 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 for sealing off any areas where an explosion or attack has occurred, available at all times. Keep key personnel who may be needed to implement security plans on call.

(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 installation and nonclassified areas under the jurisdiction of the installation or command.

(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:

22 SEP 1998

(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 other regular and frequent intervals, inspect for suspicious activity or packages on the interior and exterior of buildings in regular use. (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 deterrence and defense and build confidence among staff and dependents. (Measure 18)

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

(8) Measure 8. Review and implement security measures for high-risk personnel.

(9) Measure 9. General visitation is not authorized, which includes the flightline.

b. THREATCON BRAVO. This condition is declared when there is increased and more predictable threat of terrorist activity even though no particular target is identified. The measures of this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability or aggravating 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.

(4) Measure 13. Where possible, move cars and objects such as crates, trash containers, etc., 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.

22 SEP 1998

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

(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 build confidence among staff and dependents.

(10) Measure 19. Make staff and dependents aware of the general situation 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. On 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 per prepared plans. Remind drivers to lock parked vehicles and institute a positive system of checking before they enter and drive cars.

(15) Measure 24. Implement additional security measures for high-risk personnel.

(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, critical communication facilities/assets, etc.

(18) Measure 27. Recall Security Department and place Auxiliary Security Force in an Immediate Recall Stand-By Status. Brief Security Force personnel on threats, use of deadly force and rules of engagement.

(19) Measures 28-29. Spare.

22 SEP 1998

c. THREATCON CHARLIE. This condition is declared when an incident occurs or when intelligence is received indicating that some form of terrorist action against the installation or personnel is imminent. Implementation of this measure for more than short periods will probably create hardship and will affect the peacetime activities of the installation and its personnel.

(1) Measure 30. Continue all THREATCON BRAVO measures or introduce those outstanding.

(2) Measure 31. Keep all personnel who are responsible for implementing anti-terrorist plans available at their places of duty.

(3) Measure 32. Limit access points to an absolute minimum.

(4) Measure 33. Strictly enforce control of base entry and search a percentage of vehicles.

(5) Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.

(6) Measure 35. Issue weapons to guards (Local orders must include specific orders on issue of ammunition).

(7) Measure 36. Introduce increased patrolling of the installation to include waterfront areas, wharfs, piers, caissons, critical communication facilities/assets, drydocks, etc.

(8) Measure 37. Protect all designated vulnerable points (VPs) and give special attention to VPs outside Naval installations and activities.

(9) Measure 38. Erect barriers and obstacles to control traffic flow.

(10) Measure 39. Recall the Auxiliary Security Force immediately. Brief security personnel on threat, use of deadly force and rules of engagement.

d. THREATCON DELTA. A terrorist attack has occurred or intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

(1) Measure 40. Continue or introduce all measures listed for THREATCON BRAVO and CHARLIE.

(2) Measure 41. Augment guard and/or police forces as necessary.

22 SEP 1998

(3) Measure 42. Identify all vehicles already on the installation within operational or mission support areas.

(4) Measure 43. Search all vehicles and contents entering the complex or installation.

(5) Measure 44. Control all base access points and implement positive identification of all personnel.

(6) Measure 45. Search all suitcases, briefcases, packages, etc., brought into the installation or command.

(7) Measure 46. Control access to all areas under the jurisdiction of the Naval installation or command concerned.

(8) Measure 47. Make frequent checks of the exterior of buildings and parking areas.

(9) Measure 48. Minimize all administrative journeys and visits.

(10) Measure 49. Consult local authorities about closing public and military roads and facilities that might make sites vulnerable to terrorist attack.

(11) Measure 50. Man posts as necessary to prevent attack against vulnerable facilities outside the base boundaries (e.g., emergency power generators close to base boundary, microwave relay towers located off base, etc.).

6. 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.

22 SEP 1998

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

b. 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 and targeting must be present. History and intentions may or may not be present.

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

(4) Low. Factors of existence and capability must be present. History may or may not be present.

(5) Negligible. Factors of existence and/or capability may or may not be present.

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

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

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX G

CIVIL DISTURBANCE

1. Purpose. To establish procedures for managing civil disturbances and demonstrations.

2. Scope. The scope of this appendix applies to NAS Oceana, NALF Fentress and Navy Bombing Ranges, Dare County, NC, Palmetta Point, NC, Stumpy Point, NC and Telephone Repeater Station, Cape May, NJ.

3. Discussion. Protest organizations may express their views through passive demonstrations near government installations. However, some demonstrators have attempted to damage government property and disrupt normal operations during these events. When this situation occurs, a security response commensurate to the threat level is appropriate.

4. Responsibilities

a. Commanding Officer (CO). Deploy Security Forces against unruly civil disturbances; activate command center if necessary.

b. Command Duty Officer (CDO). Assist the CO and Security Officer; prepare OPREP-3 message.

c. NAS Oceana Quarterdeck notify CO, Public Affairs Officer and others as directed.

d. Security Officer. Designated On-Scene Commander. Direct Security Forces to quell civil disturbance; coordinate with local authorities for law enforcement support.

(1) Implement security plans and contingency response to monitor and neutralize threat on NAS Oceana and its outlying facilities.

(2) The Security Detachment Watch Commander shall notify:

- (a) Command Duty Officer (CDO).....433-2366
- (b) Security Officer433-3103
- (c) Naval Criminal Investigative Service..433-3291
- (d) Fire Department433-3333
- (e) Branch Medical Clinic677-7182
- (f) Virginia Beach Police Department427-5616

NASOCEANAINST 5330.4C

31 OCT 1997

e. Individuals having knowledge of a civil disturbance or demonstration shall notify the Security Detachment at 433-3103 or 433-2124.

f. Host Departments and Tenant Commands. Brief personnel of threat; ensure appropriate internal security measures are implemented to secure buildings and plant property from threat and stay clear of the civil disturbance or demonstration.

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX H

PHYSICAL SECURITY AND LOSS PREVENTION

1. General. Loss and Crime Prevention programs shall be implemented by all NAS Oceana and tenant commands per reference (a). A successful Loss and Crime Prevention Program requires continuous command emphasis.
2. Responsibilities
 - a. Commanding Officer. Provide sufficient resources to manage and execute an effective Physical Security and Loss Prevention Program.
 - b. Security Officer. Plan and manage the Command Physical Security and Loss Prevention Program.
 - c. Loss Prevention Officer. Implement the Command Physical Security Prevention Program.
 - d. Commanding Officer/Officers-in-Charge of Tenant Activities. The commander of each tenant activity shall implement a Physical Security and Loss Prevention Program consistent with the guidelines in this appendix.
3. Inventory Controls. Strict inventory control measures allow commands to maintain accountability for the location of items and early identification of lost items. This greatly enhances the opportunity for recovery of the missing item. Commands and departments are responsible for implementing strict inventory control system for all government property.
4. Missing-Lost-Stolen-Recovered (MLSR) Program. Loss of property requiring an MLSR report will be reported to the Security Detachment. Incidents requiring MLSR reports shall be referred to NCIS for review and investigation. Reference (d) of appendix A provides Navy and host command MLSR procedures.
5. Physical Security Survey. Provided to identify existing security measures, physical security deficiencies and areas which require improvement. Additionally, it may be used as a reference to plan and budget for future physical security issues. A survey of each department and host activity shall be conducted annually.
6. Key and Lock Control Program. Guidelines for this program are contained in reference (a). Each department and host activity shall implement a Key and Lock Control Program.

31 OCT 1997

a. Key Control Officer. Designated in writing by each Commanding Officer or Officer-in-Charge. This person shall plan and manage all organizational key and lock control procedures.

b. An annual inventory of all controlled keys, logs and records shall be completed.

c. Key Custodians appointed by the Key Control Officer shall conduct a quarterly key control inventory and review key logs for discrepancies.

d. Rotate security locks, padlocks or lock cores at least annually or when required by other instructions.

e. Develop local procedures and records for key issue accountability.

7. Crime Prevention Program. The development of command crime prevention methods will reduce the opportunity for installation criminal activity and property loss. Each Commanding Officer or Officer-in-Charge shall maintain an effective Crime Prevention Program using the following guidelines:

a. Implement a schedule for Loss Prevention meetings to discuss loss trends and preventive measures to reduce property loss.

b. Conduct annual Physical Security Surveys to identify vulnerabilities of high incident areas.

c. Publish related information in local media using PODs, flyers and questionnaires to enhance personal awareness.

d. Encourage personnel to participate in Operation Identification Programs to mark or stencil personal high value items with initials and social security numbers.

e. Implement annual command Loss Prevention training.

8. Community Policing Program. Managed by the Security Detachment to provide a safe and secure living and working environment through active involvement with every aspect of installation community. This crime prevention initiative implements proactive problem solving efforts on behalf of the Security Force and installation community. All departments and host activities are encouraged to participate in the following Community Policing Programs:

31 OCT 1997

a. Neighborhood Watch Program. Service members and their families may actively participate in protecting their community. This program consists of an organized network of citizens interacting with their neighbors and the Security Force to prevent and deter crime in their neighborhood. Law enforcement efforts are enhanced when the residents of the Navy housing areas patrol their neighborhood and notify the Security Force of crimes in progress and suspicious activity.

b. Crime Prevention Briefs. The Security Detachment shares crime prevention information to the local installation community, which enhances their personal security awareness.

c. Ident-A-Kid Program. Provides positive identification of all military dependent children by using recent photographs and fingerprints. This could be a valuable reference in the event of crimes against children.

d. Home Security Survey. Provides a no cost physical security inspection of a dwelling by Security Detachment Crime Prevention personnel to identify home security deficiencies and recommend measures to reduce building vulnerability.

e. Officer Friendly Program. Provides awareness lectures and information to gatherings of children (i.e. Pre-school, NEX, Child Care, Youth Services, etc.). Personal contact encourages children to interact with Security Force personnel in a positive manner.

f. Bicycle Rodeo Program. Provides instruction to children about bicycle safety, the rules of the road and includes bicycle registration.

g. Welcome Aboard Program. Provides information about the Community Policing Program to newly arrived families in Navy housing.

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX I

CONTROL OF PHOTOGRAPHY

1. Purpose. To control photography on board NAS Oceana and promulgate guidance in cases of unauthorized photography.
2. Privately Owned Cameras. Privately owned cameras and photographic equipment shall not be allowed in restricted areas except when authorized by competent authority and under escort.
3. Responsibility. Departments and host activities are responsible for controlling the photography of all material within their jurisdiction.
4. Unauthorized Photography. Persons detained or apprehended for unauthorized photography in restricted areas shall have all camera film and equipment confiscated; individuals shall be processed by the Security Detachment or Naval Criminal Investigative Service for further disposition.

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX J

HUNTING INFORMATION

1. Purpose. To provide general hunting information to all personnel on board NAS Oceana and NALF Fentress.
2. Scope. Applicable to all personnel who desire to hunt within the boundaries of NAS Oceana and NALF Fentress.
3. General. Per reference (v), hunting within the boundaries of NAS Oceana and NALF Fentress is controlled by the Commanding Officer, NAS Oceana. All hunters are subject to Commonwealth of Virginia and federal game laws and are required to purchase the appropriate State or County licenses in addition to a station permit to hunt or fish on board the station. The station Wildlife Officer shall enforce all state and federal game laws within station boundaries.
 - a. Hunting Qualifications. Before obtaining a station hunting permit all hunters are required to complete a state certified hunter safety course. Bowhunters must show proof of completion for the International Bowhunter Education Program (IBEP) and successfully complete a proficiency test with the same equipment used for hunting. Additionally, a base hunting indoctrination conducted by the Natural Resources Manager is required.
 - b. Hunter Eligibility
 - (1) Active duty, reserve and retired military personnel.
 - (2) Civilian personnel employed at NAS Oceana.
 - (3) Eligible personnel may sponsor guests to hunt on station provided they meet all qualifications and requirements. Guests shall be accompanied by their sponsor at all times while hunting on station. Sponsors are reminded that they are responsible and will be held liable for guest's actions while hunting.
 - c. Hunter Check-in/out Procedures. Hunters are required to abide by check-in and check-out procedures with NAS Oceana Security, Building 320 or NALF Fentress Crash Captain's Watch, Building 100. Hunters may check out a hunting area two hours prior to sunrise and must be checked out no later than two hours after sunset.

31 OCT 1997

d. Hunting Seasons. Hunting seasons shall coincide with state and federal game seasons. The only game animals that may be harvested during their prescribed season are morning dove, squirrel, rabbit and deer.

e. Safety. Clothing with 100 square inches of international blaze orange is required to be worn by all hunters during any state deer firearms season. Once on stand, NAS Oceana bowhunters can remove blaze orange and display at shoulder level within arms reach and visible from 360 degrees. Hunters at NALF Fentress and all small game hunters are required to wear blaze orange while hunting.

PHYSICAL SECURITY PLAN

APPENDIX K

BUILDING SECURITY

1. Purpose. To provide guidance for the physical security of buildings, compounds and perimeters.
2. Scope. This applies to all buildings and fences on board NAS Oceana; NALF Fentress; Bombing Ranges, Dare County and Stumpy Point, NC and Telephone Repeater Station, Cape May, NJ.
3. Security of Buildings
 - a. Departments and host activities are responsible for the internal security of the structures and facilities they occupy.
 - b. Key and Lock control guidance is contained in appendix H of this instruction.
 - c. All NAS Oceana buildings and spaces shall be secured at the close of the normal workday and any time when not occupied. Unnecessary utilities, external doors, windows and other openings which could provide access shall be secured.
 - d. Individuals assigned to work in buildings or spaces after normal working hours shall ensure access to their areas are secured.

31 OCT 1997

PHYSICAL SECURITY PLAN

APPENDIX L

CRISIS ACTION RESPONSE PLAN

1. Purpose. To identify Crisis Response Forces (CRF) and provide security guidance for response actions to disasters, subversive and criminal acts and terrorist activities on board NAS Oceana per references (u) and (w).
2. Background. Periods of routine security posture, criminal, subversive, terrorist incidents and disasters may require the implementation of special crisis response plans. Public safety, containment and capture of the perpetrators are the CRF objectives.
3. Responsibilities
 - a. Crisis Response Force Commander. The Commanding Officer of Naval Air Station Oceana or his direct representative is responsible for the overall security of the installation.
 - b. On-Scene Commander. The Security Officer shall assume the duties as On-Scene Commander and keep the Commanding Officer appraised of the incident. The On-Scene Commander is responsible for the field management and training of the CRF.
 - c. On-Scene Tactical Commander. The Security Detachment Operations Division Officer is responsible for the employment and direction of all operational and supplemental security forces and local authorities support.
4. Crisis Response Force (CRF)
 - a. The NAS Oceana CRF consists of the Security Detachment and Auxiliary Security Force (ASF). Personnel assigned to the CRF shall be trained and equipped to react, contain and deter criminal, subversive and terrorist acts. Additionally, the CRF shall be capable of responding to disaster preparedness incidents.
 - b. The Security THREATCON measures in Appendix F of this instruction provide defense readiness guidance applicable to all crisis incidents on board NAS Oceana. These THREATCONS, when partially or fully implemented with the activation of the CRF, will provide an acceptable security posture commensurate to any threat.

81 OCT 1997

5. Other Local CRF Support Elements

- a. NAS Oceana Fire Department
- b. NAS Oceana Branch Medical Clinic
- c. Construction Battalion Unit (CBU-415)
- d. NAS Oceana Public Works Center
- e. EOD Group Two Detachment, Norfolk
- f. NCIS Oceana Resident Agents
- g. Virginia Beach Police Department
- h. Fleet Antiterrorist Support Team Company, Marine Corps Security Force Battalion Atlantic. This unit may be requested from Commander-in-Chief, U.S. Atlantic Fleet via Chain-of-Command.
- i. Commander, Naval Base Norfolk. The Regional Area Coordinator will be the point of contact for requesting additional Crisis Response Force support.

6. Action. On notification of an impending incident requiring the CRF on board NAS Oceana, the following actions shall be considered:

- a. Commanding Officer. Ensure chain-of-command is notified; may activate the primary Command Center, Building 232, to implement command and control crisis management procedures, recall appropriate Command Center staff personnel and increase installation security measures. The alternate Command Center site is the NAS Oceana Quarterdeck in Building 230.
- b. Security Detachment. Deploy security forces commensurate to the threat, establish an on-scene Mobile Command Post and maintain the appropriate armed security perimeters to contain the incident. Activate the Auxiliary Security Force as needed, notify the Naval Criminal Investigation Service Resident Agency and the Virginia Beach Police Department.
- c. Naval Criminal Investigation Service (NCIS). Coordinate intelligence gathering, provide threat assessment briefs and manage hostage negotiation incidents. Additionally, NCIS will coordinate with the Federal Bureau of Investigations (FBI) to employ on jurisdiction matters and the use of special tactical assault assistance if needed.

31 OCT 1997

d. Supply Officer. Provide emergency berthing and rations for Security Force personnel.

e. Base Civil Engineering Officer. Coordinate heavy equipment and logistics support with Public Works Center Oceana and Naval Construction Battalion Unit 415 as required.

f. Air Operations Officer. Provide Firefighting support.

g. NAS Oceana Branch Medical Clinic. Provide ambulatory and other medical assistance.