



DEPARTMENT OF THE NAVY

UNITED STATES NAVAL ACADEMY

121 BLAKE ROAD

ANNAPOLIS, MARYLAND 21402-5000

USNA/AACINST 5530.2A
4/SECOFCR

15 November 2000

USNA/AAC INSTRUCTION 5530.2A

From: Superintendent, U.S. Naval Academy/Annapolis Area Coordinator

Subj: PHYSICAL SECURITY PROGRAM

Ref: (a) OPNAVINST 5530.14C
(b) USNAINST 5512.7A
(c) BKS P5500.3 (NOTAL)
(d) NAVY REGULATIONS
(e) SECNAVINST 1740.2D
(f) USNAINST 1741.2D
(g) USNA/AACINST 5560.7C
(h) USNAINST 5500.9
(i) OPNAVINST 5580.1A
(j) USNAINST 3440.3
(k) USNAINST 3440.1F
(l) OPNAVINST 5585.2B
(m) USNAINST 5800.2A
(n) USNAINST 5800.3
(o) DODDir 5200.8
(p) OPNAVINST 3300.54
(q) OPNAVINST 3300.55
(r) NCIS 28SEP00-DCAN-0069-5GNA/C (NOTAL)

Encl: (1) Force Protection Plan
(2) Department of the Navy Telephonic Threat Complaint Form (OPNAV 5527/8)

1. Purpose. To provide a guide to U.S. Naval Academy (USNA) policies and procedures of physical security, per references (a) through (r).
2. Scope. Enclosure (1) addresses physical security responsibilities and minimum criteria for the protection of property and personnel. It is applicable to USNA and tenant activities of USNA Annapolis.
3. Cancellation. USNAINST 3440.1F and USNA/AACINST 5530.2. This directive is a complete revision and should be reviewed in its entirety. No special markings appear because changes are extensive.
4. Responsibilities. Physical Security is the direct, immediate, legal, and moral responsibility of all personnel assigned to this installation.

a. The Command Security Officer is the designated representative of the Superintendent, USNA, and is responsible for planning, implementing, enforcing, and supervising the Physical Security Program for this installation.

b. All Cost-center Heads and tenant activity directors are responsible for implementing this instruction to include checking for compliance throughout subordinate activities.

5. Forms Availability. Forms listed in enclosure (1) are available through the Security Department.

M. E. McWATTERS
Deputy for Operations

Distribution:
AA

For Official Use Only

15 November 2000

TABLE OF CONTENTS

<u>Contents</u>	<u>Page</u>
JURISDICTION	1-1
Situation	1-1
Mission	1-1
Application	1-1
SECURITY AREAS	2-1
Purpose	2-1
Authority	2-1
Restricted Area	2-1
Control Measures	2-1
PERSONNEL ACCESS, IDENTIFICATION, AND MOVEMENT	3-1
Purpose	3-1
Definitions	3-1
General Policy	3-1
Debarment from the Installation	3-4
Station Badge and Pass	3-5
VEHICLE ACCESS, IDENTIFICATION, AND MOVEMENT	4-1
Purpose	4-1
Scope	4-1
General Policy	4-1
Government Vehicles	4-1
Responsibilities	4-1
Categories of Commercial Vehicles	4-2
Motor Vehicle Registration and Driver Records	4-2
Barge control	4-2
MATERIAL CONTROL	5-1
Purpose	5-1
Responsibility	5-1
SEIZURE AND HOLDING OF CONTRABAND PROPERTY/EVIDENCE	6-1
Purpose	6-1
Contraband Property	6-1
Prohibited Property	6-2
Seizure of Property	6-3
INTERNAL SECURITY	7-1
Purpose	7-1
Procedures	7-1
Security of Buildings	7-1
AIDS TO SECURITY	8-1
Situation	8-1
Control	8-1
Type of Aids	8-1

15 November 2000

<u>Contents</u>	<u>Page</u>
Security Force	9-1
Purpose	9-1
Mission	9-1
Organization	9-1
Weapons and Equipment	9-3
Training	9-4
Use of Sentry/Patrol Dogs	9-4
Auxiliary Security Force (ASF)	9-4
Marine Barracks Annapolis	9-6
CRISIS MANAGEMENT	10-1
Situation	10-1
Mission	10-1
Execution	10-1
Appendix A (THREATCONS)	A-1
Purpose	A-1
Threat Assessment	A-1
Collection, Analysis and Distribution of Terrorist Threat Information ..	A-2
General	A-2
Threat Assessment Guidelines	A-7
Enclosure (1) Barricade Plan	A-9
Appendix B (CIVIL DISTURBANCE)	B-1
Situation	B-1
General	B-1
Execution	B-1
Responsibilities	B-4
Appendix C (HOSTAGE SITUATION)	C-1
Purpose	C-1
General	C-1
Mission	C-1
Execution	C-1
Responsibilities	C-2
Appendix D (SABOTAGE)	D-1
Purpose	D-1
General	D-1
Mission	D-1
Execution	D-1
Appendix E (BOMB THREATS)	E-1
Purpose	E-1
General	E-1
Mission	E-1
Execution	E-1
Responsibilities	E-3

15 November 2000

Contents

Page

Appendix F (WEAPONS OF MASS DESTRUCTION) F-1
 PurposeF-1
 GeneralF-1
 MissionF-1
 ExecutionF-1
 ResponsibilitiesF-1

Appendix G (TRAINING) G-1
 PurposeG-1
 GeneralG-1
 MissionG-1
 ExecutionG-1

Appendix H (EMERGENCY OPERATIONS CENTER) H-1
 PurposeH-1
 GeneralH-1
 ExecutionH-1

15 November 2000

JURISDICTION

1. Situation. This annex outlines the jurisdiction of property owned by the Department of the Navy (DON) and USNA, which is defined as proprietorial interest. This means DON has acquired title to ownership to the installation but not legislative jurisdiction. The Federal government and departments and agencies thereof have authority to enact and enforce laws for the protection of U.S. Government property and the right to perform the functions delegated to it by higher Federal authority without interference from the state. For the purpose of this instruction, all property owned by the DON, operated and controlled by USNA, will be considered exclusive jurisdiction.

2. Mission. Exercise those security measures necessary to protect life, property, and use USNA security resources for crisis management while maintaining mission capability.

3. Application

a. The jurisdiction of the Superintendent over all military personnel (officers, enlisted, and midshipmen) on USNA is established by the Uniform Code of Military Justice (UCMJ) and the Manual of Court-Martial (MCM). The authority of the Department of Defense (DOD) Police, Marine guards, and master-at-arms to enforce military laws, orders, and instructions, by apprehension if necessary, is derived primarily from the Constitutional power of the President as Commander-in-Chief of the Armed Forces and the power of Congress to make rules for the Armed Forces (Article 7 UCMJ and MCM, paragraph 19a).

b. The Superintendent can enforce local and criminal laws via the Assimilated Crimes Act and exercise administrative control over civilians on USNA. The Superintendent can legally:

(1) Have civilians removed from the installation by use of reasonable force.

(2) If necessary, bar any civilian from entry into the installation for good cause.

(3) Limit access to the installation to those having legitimate necessity for entry.

(4) Limit and regulate items permitted to be brought on the installation by those permitted entry.

(5) Have individuals and vehicles entering, leaving, or staying on the installation inspected per reference (m).

c. The Superintendent's control of situations that may arise may be extended by the use of the following security organizations:

(1) DOD Police (composed of Civil Service employees).

(2) U.S. Marine Corps Personnel.

(3) Auxiliary Security Force (composed of military personnel).

USNA/AACINST 5530.2A

15 November 2000

(4) Naval Station (NAVSTA) Security Force.

d. This jurisdiction is applicable to all civilians regardless of employment status (Federal employee, contractor, or civilian).

15 November 2000

SECURITY AREAS

1. Purpose. To establish control on designated security areas.
2. Authority. Areas designated by the Superintendent, USNA, pursuant to lawful authority and published pursuant to reference (o) Section 21, Internal Security Act of 1950. Guidance for establishing controls for security is provided by reference (a). USNA tenant commands will designate and control access to security areas as required.
3. Restricted Area
 - a. Communications Center, Administration Bldg. #121, Room 10. Restricted to personnel with a secret clearance and a need to know when processing message traffic.
 - b. Security Vault, Public Safety Building #257, Room 306
 - (1) Restricted to security management personnel only and is controlled by the Security Manager.
 - (2) Requires a Secret clearance and a need to know basis.
4. Control Measures. Admission will be limited to persons whose duties require access and who have been granted appropriate authorization. Persons who have not been cleared for access to the security interest contained within the secure area are not to be admitted. The controlling authority may authorize admittance to the area for maintenance or other authorized purposes. However, those requiring admittance must be escorted at all times and the security interest protected from compromise.
 - a. Authority for access will be determined by the Officer-in-Charge (OIC) or manager of the restricted area.
 - b. Access Criteria
 - (1) Assigned personnel will be on an access roster signed by the OIC or manager of the restricted area.
 - (2) An individual assigned to the restricted area while maintenance is performed should escort maintenance personnel working in a restricted area.
 - (3) Contractor personnel to be admitted to the area are subject to approval of the OIC or manager and should be escorted by an individual assigned to the area.

15 November 2000

PERSONNEL ACCESS, IDENTIFICATION, AND MOVEMENT

1. Purpose. To prescribe policies, responsibilities, and procedures for the access, movement, and identification of individuals employed, stationed, or visiting USNA. This annex is applicable to all persons entering, while on, and departing the installation.

2. Definitions

a. Visitor. For the purpose of this instruction, definitions of visitors are contained in reference (b) with the following additions:

(1) Commercial vendors/deliveries. Individuals delivering material or services to activities on this installation.

(2) Contract personnel. Any individual working for a contractor whose contract is yearly and whose work site is on the installation.

(3) Official Visitors. Individuals from other government installations or activities visiting in an official capacity.

b. Badge. A security identification card conforming to the design and physical specifications prescribed in reference (a), chapter 5, Personnel and Vehicle Movement Control.

c. Public Areas. The USNA Annapolis is considered a Naval facility, college, and a national landmark, therefore, all areas are considered open to the public daily from 0600 to 2300 with the exception of Bancroft Hall, Administration Building #121, government quarters, and academic buildings.

3. General Policy

a. Identification

(1) All military personnel, civilian employees, eligible retired USNA faculty members, vendors, and contract personnel will be properly identified by security badges or other acceptable identification. Movement of all persons on the installation will be strictly controlled as prescribed herein.

(2) Entry into this installation will only be through Gate #1 (Main Gate), Gate #3 (Maryland Avenue and Hanover Street), and Gate #8 (Maryland Highway Route 450).

(3) The Security Department and guard force will differentiate between the permission for the entrance of vehicles and permission for persons to enter onto the installation. Permission for one does not automatically mean permission for the other. Vehicles and persons are separately controlled and separately granted entry.

b. Employees

(1) Employees will not be permitted entry onto the installation without an escort who is a resident or in a duty status after 2300 and before 0600 except for the performance of duty or the conduct of official business. Reference (b) offers detailed guidance.

15 November 2000

(2) Civilian employees of USNA and tenant commands must carry a valid Civilian Identification Card at all times. Employees will be issued a valid card by the Security Department.

(3) Active duty military personnel must carry a valid Armed Forces Identification Card, DD Form 2N, at all times.

(4) Dependents and children of military personnel employed at USNA must carry a valid Uniformed Services ID and Privilege Card, DD Form 1173, at all times on the installation. Children below the age of 10 years must be accompanied by an adult (sponsor or dependent with a valid identification card).

(5) Civilian employees of tenant activities and agencies must carry a valid identification card issued by their employment agency or the Security Department, USNA.

(6) Contract employees under contract with USNA or tenant commands will be issued identification by the Security Department on an annual basis. Short term contractors (less than 2 weeks) will not be issued ID cards as long as work is to be conducted during working hours.

(7) Security Department must be notified by a department head or activity head when contractor overtime work is to be performed after 1800, Monday through Friday, and on weekends. Notification of the number of employees working will be made as soon as possible after it has been determined overtime will be worked.

(8) All civilian identification cards will be displayed above the bearer's waist, either by a clip device or neck chain.

c. USNA Visitors

(1) Official Visitors

(a) Law enforcement and investigative agents or representatives of civil or military enforcement or investigative agencies will be admitted to USNA upon presentation of satisfactory identification. Such agents will not proceed with any official activity until the purpose of the visit has been evaluated and the Security Officer, Chief of Police, or Assistant Chief of Police have been advised. On approval from one of the above, the agent will be directed to the Staff Judge Advocate (SJA) Office for review of the documents. Naval Criminal Investigative Service (NCIS) Agents assigned to USNA are excluded from this requirement.

(b) If the purpose of the visit is to serve a civil process, warrant, or subpoena, permission to do so must be granted by the SJA. The actual service must be made per all applicable laws and on approval by the SJA. Security personnel of the USNA will accompany the agent for service of the documents.

(c) If the purpose of the visit is other than to serve a civil process, warrant, or subpoena, the activity must be coordinated with the command through the Security Officer.

15 November 2000

(d) Law enforcement officers in uniform will not be stopped from entering the installation while in fresh or hot pursuit. Security personnel will respond and obtain verifying information. If specifically requested, security personnel will aid the officers. During duty hours and in any occupied areas, the primary responsibility of the security personnel will be to safeguard personnel in the area from harm and to close off areas as required.

(e) Individuals from the government installation or activities visiting in an official capacity will be allowed entry upon presentation of a valid identification card/badge. The identification media must have a current photo affixed and contain identifying information. If prior notice has not been received by security, the department head or division head of the area to be visited will be called to verify the visit is official and is authorized.

(f) Noncitizens of the United States: Visits by foreign nationals (only identified if vehicle displays diplomatic plates) will be stopped by the Marine Guard per chapters 5 through 9 of reference (c).

(g) Affiliated union representatives conducting official business, who are not employees as defined here, will be admitted only after clearance through the civilian personnel representative. Contractor union representatives will be admitted only after clearance through the Resident Officer-in-Charge of Construction.

d. Business Visitors

(1) The basic regulations for the control of commercial solicitation aboard a Naval installation are contained in Article 0715 of reference (d) and in reference (e). These regulations provide that entrance to USNA Annapolis by solicitors and agents for the purpose of conducting public business is generally permissible. Entrance on the installation including the housing area for the purpose of conducting private business will be strictly controlled by the Superintendent, Security Officer, and Purchasing Department.

(2) Since all individuals of the installation generally have sufficient opportunity for conducting business during off duty hours, solicitors and agents of commercial concerns will not be permitted to enter the installation for the purpose of conducting private business or contracts with individuals on duty. Many military personnel live on the station and may receive representatives of that commercial concern on private business after their duty hours. Such visits will be controlled as prescribed by reference (f).

(3) Contractor personnel will be processed and approved for admission to USNA by the Security Office on a Vehicle/Visitor Pass (NDW-USNA-DMC-5560/07 (01-86), for the vehicle(s). The Vehicle/Visitor Pass will be valid only for the period of the contract.

(4) Visitors in the following categories will be admitted only after clearance by the Superintendent, or representative of the Superintendent (Naval Academy Duty Officer, Deputy for Operations, Public Affairs Officer, Security Officer):

(a) Representatives of news agencies.

15 November 2000

(b) Photographers, professional and freelance. This does not apply to general visitors (tourists, resident's guests, midshipman family, and guests, etc.).

e. General visitors. General visitors to USNA, Annapolis will be admitted per reference (b).

f. Tenant activity visitors. Tenant activity visitors are general visitors and will also comply with reference (b).

4. Debarment from the Installation

a. Individuals may be barred by the Superintendent, Commandant of Midshipmen, or the NAVSTA Commanding Officer. Individuals who are barred will not be permitted to enter the installation. Persons will not be allowed entrance based on the following circumstances:

(1) Persons who show evidence of being under the influence of alcohol or drugs will not be admitted to the installation. Notwithstanding any of the provisions for admission to the installation contained in this annex, no person will be allowed to enter or exit the installation that is suspected of being under the influence of alcohol or drugs.

(2) Individuals visiting employees for purely personal reasons without the express permission of the area supervisor or department head will not be allowed entry onto the installation.

(3) Peddlers, solicitors, creditors, re-possessors, and other like categories of individuals, except when specifically authorized by the Superintendent, will not be allowed entry onto the installation.

(4) Individuals participating in picketing, demonstrations, sit-ins, protest marches, political speeches, and similar activities will be cause for removal and debarment from the installation.

(5) Distribution on the installation of material such as pamphlets, handbills, flyers, newspapers, magazines, leaflets, petitions, etc. is prohibited except through regularly established and approved distribution outlets or unless prior approval is obtained from the Superintendent.

(6) Offensive or degrading signs, placards, or stickers, whether hand carried, affixed to, or painted upon buildings, conveyances, or other objects, are prohibited.

(7) No one will enter or remain on this installation for any of the purposes prohibited by this instruction. Such entry will constitute a violation of Title 18, United States Code, Section 1382, which provides in part: "whoever, within the jurisdiction of the United States, goes upon any military reservation station or installation, for any purpose prohibited by law and lawful regulation will be fined not more than \$500.00 or imprisoned not more than 6 months, or both."

b. Procedures used to issue a debarment letter

15 November 2000

(1) All bar letters will be issued by the Superintendent, Commandant of Midshipmen, or the Commanding Officer NAVSTA, USNA Annapolis.

(2) Bar letters will specify the reason for the action.

(3) The individual barred may submit a written request to the Deputy for Operations USNA, or NAVSTA Executive Officer for reconsideration or modification of the barment action. A record of the decision upon reconsideration will be maintained on file in the SJA office.

5. Station Badge and Pass

a. Station Identification Badges

(1) Civilian Identification Cards (NDW-USNA-DMC-5512/01) are issued at the Pass and Tag Office per chapter 5 of reference (a). This applies to:

(a) All civil service employees.

(b) Retired USNA faculty members with at least 20 years faculty service at the Naval Academy; or a combined total of at least 20 years of military, government, and Naval Academy faculty service.

(c) Permanent and temporary contractors.

(2) Vehicle DOD decals and Temporary Visitor Parking Permits (NDW-USNA-DMC-5560/07) are issued at the Pass and Tag Office. This applies to all residents, employees, midshipmen, eligible retirees, and permanent and temporary contractors.

(3) Upon termination of duty, employment, or contract, the respective individual is required to report to the Pass and Tag Office for the turn in of all identification media (employees' identification card and vehicle decal scrapings, when appropriate).

(4) Employees separating by mail or abandonment of position will be directed to mail Civilian Identification Cards, Vehicle DOD decals, and Visitor Parking Permits to USNA, Annapolis. Clearance of the individual will be withheld until all cards and decals are returned. Employees who do not return their identification cards, which remain U.S. Government property, are subject to the penalties prescribed under Title 18, United States Code 506, 449, and 701.

b. Lost, Stolen and Forgotten Station Identification Cards. Each individual to whom an identification card has been issued must immediately report the loss or theft of such card to his/her department head or Resident Officer-in-Charge of Construction in the case of a contractor.

(1) The department head will issue a letter to the Pass and Tag Office so a new card can be issued immediately.

(2) If an individual forgets their identification card, they will notify their department head. During increased security posture they will have someone from their office escort them onto the Yard. Any necessary action will be at the discretion of the department head.

15 November 2000

(3) The Pass and Tag Office clerk will assure the serial numbers of all lost badges are posted at the Pass and Tag Office and all manned posts.

c. Standards for Replacement of Badges

(1) Station identification cards will be issued for a period not to exceed 3 years to all civilian employees of USNA, Annapolis.

(2) Identification cards will be issued for a period not to exceed 1 year or the length of their contract to all contract employees and service representatives of USNA, Annapolis.

(3) When a loss level of six percent of the total station identification cards has been reached, all security identification badges must be invalidated and new badges issued.

15 November 2000

VEHICLE ACCESS, IDENTIFICATION, AND MOVEMENT

1. Purpose. To prescribe policies, responsibilities, and procedures applicable to public, commercial, and military vehicles while entering and operating on the installation are governed, in part, by the provisions of this chapter.

2. Scope. This annex is applicable to all persons entering, while upon, and while departing the installation. All motor vehicles, motorcycles, and bicycles operating on the installation are governed, in part, by the provisions of this chapter.

3. General Policy

a. All self-propelled motor vehicles operating on the installation after visiting hours must be identified by DOD decal or visitor pass. Government-owned or leased vehicles and contractor industrial construction equipment; e.g., cranes, drag lines, earth movers, tractors, and other self-propelled equipment used at the job site are exempt from this requirement.

b. The display of a valid registration (decal) does not constitute automatic entrance to the installation for the occupants. The occupants must meet the requirements of chapter 3 of this instruction.

c. Persons operating motor vehicles, scooters, and bicycles on the installation will comply with the provisions of the vehicle and traffic regulations as set forth in reference (g).

4. Government Vehicles

a. All U.S. Government-owned or leased vehicles assigned to USNA will be allowed off base and exit without delay.

b. Government vehicles assigned to other U.S. Government agencies or installations will be admitted to the station when the occupants have satisfied the requirements for entry as set forth in chapter 3 of this instruction. All U.S. Government vehicles making pickups or deliveries to activities of this installation will comply with the consignee vehicle controls as stated.

c. Persons operating motor vehicles assigned to USNA off station will comply at all times with the State of Maryland Vehicle Code.

d. Government vehicles will not enter privately owned vehicle (POV) parking lots or stop near POV parking lots unless on official business that requires access to the POV parking areas.

5. Responsibilities

a. The Security Officer is responsible for:

(1) Developing and enforcing regulations and instructions governing the operation of vehicles on the installation.

(2) Providing for the registration of private motor vehicles being operated on the installation.

15 November 2000

(3) Maintaining current files identifying all POVs registered on the Installation.

(4) Establishing enforcement measures for traffic regulations and instructions.

(5) Initiating the investigation of all vehicle accidents on the installation.

(6) Initiating action, through the Public Works Department, for posting and removal of traffic signs and other control devices.

b. Cost-center Heads are responsible for:

(1) Disseminating vehicle restrictions and limitations.

(2) Taking appropriate disciplinary action against violators reported by the Security Officer.

c. Individuals subject to this instruction are responsible for:

(1) Understanding and complying with this instruction and chapter.

(2) Proper operation of POVs within the installation by those they sponsor for entry.

6. Categories of Commercial Vehicles. Commercial vehicles entering the installation will be divided into two categories as follows:

a. Consignee Vehicles. This category includes all commercial vehicles entering the installation for the purpose of making consignee pickups or deliveries of property.

b. Vendor Vehicles. This category includes vehicles entering the installation for the purposes of making deliveries or pickups of goods at the Officers' and Faculty Club, USNA Store, Midshipmen Welfare and Recreation Facilities, Naval Academy Athletic Association (NAAA), and government quarters. Service and utility representatives' vehicles are considered vendors for the purposes of this instruction.

7. Motor Vehicle Registration and Driver Records

a. Vehicle registration and procedures for and registration of motor vehicles will be per reference (b).

b. Termination of registration will be per reference (b).

c. Pass and identification records of motor vehicles will be maintained by Pass and Identification Section, Security Department, USNA, per reference (b).

8. Barge control

a. The arrival of all barges will be recorded on the Security Journal. It will include the following information:

15 November 2000

(1) The tug number and/or name, the skipper's name, and the name of the tug company.

(2) The number of barges involved.

(3) The time of arrival and departure of the tug.

b. The activity or department concerned will be notified by the Security Officer on the first workday after the arrival of the barge(s).

15 November 2000

MATERIAL CONTROL

1. Purpose. To establish control and procedures for incoming materials.

2. Responsibility

a. Control

(1) The control of incoming material will be the responsibility of the individual department/cost center to whom the material is being delivered.

(2) The only exception is when dealing with hazardous material when prearrangements have been made with the Security Department and Fire Department for escort.

b. Admission

(1) Incoming material being delivered during NORMAL and ALPHA THREATCONS will be directed to the building the material is being delivered to.

(2) Incoming material being delivered during THREATCON BRAVO, CHARLIE, and DELTA will be:

(a) Directed to the Perry Center Complex where the vehicle will be searched by Security Force and Supply Department personnel for explosives, contraband, etc.

(b) Verification of the Bill of Lading.

(c) Inspection of operator's credentials and identification of any passengers.

(d) Contact department/cost center where the material is being delivered, for escort personnel from department/cost center.

(e) The operator of the vehicle will be issued a special vehicle pass and directed to Gate # 8 for entry to the Naval Academy.

15 November 2000

SEIZURE AND HOLDING OF CONTRABAND PROPERTY/EVIDENCE

1. Purpose. Declares and defines property considered contraband and prohibited to possess on the installation. Establishes policies governing seizure and disposition of property. Applies to all individuals on the installation.

2. Contraband Property. Property which is defined by Federal/state statute as illegal to possess and subject to forfeiture upon lawful seizure. The following items are contraband property on USNA, Annapolis.

a. Controlled Substances. A drug or other substance included in schedule I, II, or III, established by section 202 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (84 stat 1236), as updated and published under the provision of the Act in the Code of Federal Regulations and for which a valid doctor's prescription is not in immediate possession.

b. Drug Abuse Paraphernalia. All equipment, products and materials of any kind which are used, intended for use, or designed for use in injecting, ingesting, inhaling, or otherwise introducing into the human body, marijuana, a narcotic substance, or other controlled substance in violation of the law. It includes:

(1) Hypodermic syringes, needles, and other objects used, intended for use, or designed for use in introducing controlled substances into the body, and metallic or other containers used for mixing or other preparation of heroin, morphine, or other narcotic substances prior to injection.

(2) Objects used, intended for use or designed for use in the ingesting, inhaling, or otherwise introducing marijuana, cocaine, hashish or hashish oil into the human body, such as:

(a) Roach clips; meaning objects used to hold burning material, such as a marijuana cigarette that has become too small or too short to hold in the hand.

(b) Chamber pipes, carburetor pipes, electric pipes, air driven pipes, chillums, bongs, ice pipes or chillers and other pipes, with or without screens, hashish heads, or punctured metal bowls, designed for the purpose of smoking marijuana or hashish.

(c) Cocaine and heroin spoons.

c. Marijuana and Cannabis. The botanical name for a genus of plants commonly referred to as marijuana.

d. Counterfeit Currency. Any copy, photo, or other likeness of any U.S. currency either past or present not authorized by the U.S. Treasury Department.

e. Pyrotechnics and Fireworks. Any explosive or incendiary substance or devices not specifically authorized by license/military use.

f. Blackjacks, billy club, metal knuckles, and similar weapons.

15 November 2000

g. Gambling Equipment. Equipment defined by the Maryland Penal Code as unlawful to possess as gambling equipment.

h. Obscene, seditious or espionage materials.

i. Property in Illegal Possession. Any property, private or government, in the possession of an individual illegally.

3. Prohibited Property. Property other than contraband, the possession of which is prohibited by order of the Superintendent or by instruction/regulation/directive. The following items are prohibited on this installation:

a. Alcoholic Beverages. The possession and the use of alcoholic beverages by any person on the USNA, Annapolis is prohibited except as provided below. Minors may not under any circumstances purchase, possess, or consume alcoholic beverages on USNA, Annapolis.

(1) Alcoholic beverages may be consumed within the confines of the Officers' and Faculty (O&F) Club, NAVSTA location, and all station quarters and housing.

(2) Alcoholic beverages may be dispensed or consumed in other areas only with the approval of the Superintendent.

b. Firearms. The possession, carrying, and keeping of weapons on USNA is strictly forbidden except as stated below:

(1) Security force personnel are authorized to carry and use firearms in the performance of their assigned duties.

(2) Agents or representatives of civil or military law enforcement and investigative agencies will be admitted to the station and allowed to carry their weapons if they are on official duty.

(3) Military personnel who reside in government housing on USNA, Annapolis may keep firearms in their homes provided such arms are registered with the Security Office. These weapons will not be carried on the station except when being transported unloaded between the owner's home and an off-station location or on the station when going to and from authorized hunting areas and ranges.

(4) Range Control. Bancroft Hall Indoor Rifle and Pistol Range is the responsibility of and under the control of the Commandant of Midshipmen/NAAA. Members and authorized guests are not authorized to carry weapons and ammunition (ammo) to and from the range. All weapons and ammo used on this range are stored at the Bancroft Hall Armory. The Naval Station Armory and Ranges are under the control of NAVSTA Annapolis.

(5) Hunting/Hunter Control. No hunting or shooting is permitted at USNA, Annapolis except as defined in paragraph 3b(3) and (4). No hunting is authorized. The security force is responsible for responding to required police/security situations that may occur at the USNA Dairy Farm, Gambrills, MD.

c. Tear Gas. The possession, carrying, and keeping of tear gas canisters; i.e., mace, curb, etc. by other than law enforcement personnel on duty and as part

15 November 2000

of their issued equipment is prohibited. Civilian permits to carry tear gas are not recognized on this installation.

d. Knives. Knives with a fixed/folding blade longer than four inches will not be carried by individuals either concealed or openly. Contractors and employees whose duties require such a knife will be permitted to use the knife on the job but not carry it attached to the person other than at the job site.

e. Photographic Equipment. All photographic equipment is prohibited within the confines of the Communications Center, Building 121, Room 10, and the Security Manager's Vault located in Building 257. Only photographs for official use may be taken in these facilities and only by the assigned photographer as authorized by the Superintendent.

f. Citizens Band/Amateur Radio Equipment. The installation and/or operation of any citizen band/amateur radio (stationary) equipment within the limits of the installation is prohibited except as authorized by the Superintendent. Mobile citizens band/amateur radios and telephones are not restricted by this instruction. Commercial broadcasting equipment is also prohibited except by authorization of the Superintendent. Federal Communication Commission regulations must be adhered to as applicable.

g. Promotional Material. The possession, display, or distribution/sale of promotional material relating to controlled substance; i.e., T-shirts, posters, jewelry, bumper stickers is prohibited on the station.

h. The above definitions of contraband and/or prohibited property do not apply to items received into or shipped from the installation/tenant activity mission stock or operating supplies.

4. Seizure of Property

a. Security personnel will seize contraband and/or prohibited items when possessed in violation of instructions or statute, when incidental to the lawful detention or apprehension of an individual, or when necessary to prevent the commission of an offense. Action will be taken as follows:

(1) Security personnel will list and properly mark the property for identification immediately upon seizure, impoundment, or both. Marking will be scratched on the surface or otherwise affixed on the item seized or impounded so as to make the item distinguishable from other like or similar objects. This will be done in the presence of the person from whom it was seized and in the presence of a third person as a witness if possible.

(2) All property acquired as evidence by security personnel will be processed in accordance with reference (i).

(3) Items not required for evidence will be destroyed.

15 November 2000

INTERNAL SECURITY

1. Purpose. To prescribe policies, responsibilities, and procedures for the operation and maintenance of the installation key and lock control system and for the physical security plan of buildings.
2. Procedures. Tenant activities and agencies (except all Naval) will comply with their own key and lock control procedures. They may voluntarily turn keys into the USNA depository; however, all tenant activities and agencies that turn keys into USNA, Annapolis key depository must comply with the station key and lock control program.
3. Security of Buildings
 - a. All structures and facilities of the installation are assigned to USNA departments or tenant activities and agencies for their use.
 - b. Each department or tenant activity has the primary responsibility for internal security of the structures and facilities assigned to them.
 - c. Each department head and tenant activity director or head is responsible to enforce internal security of building regulations in their assigned areas.
 - d. USNA, Security Police will patrol all common areas (streets, roads, etc.) and inspect the external structures and facilities. All violations will be reported to cost center heads by Security Police.

15 November 2000

AIDS TO SECURITY

1. Situation. A viable security program will rely on various types of aids to enhance the security program. The program is multi-faceted using alarms, barriers, gates, signs, lighting, and communications. These aids are used continuously and increased at certain security levels depending on the situation.

2. Control. The type and use of security aids is determined by the Security Officer, USNA.

3. Type of Aids

a. Protective Barriers. Physical barriers control, deny, impede, delay, and discourage access to restricted and nonrestricted areas by unauthorized persons. They accomplish this by:

(1) Defining the perimeter of restricted and nonrestricted areas.

(2) Establishing a physical and psychological deterrent to entry as well as providing notice that entry is not permitted.

(3) Enhancing detection and apprehension opportunities by authorized personnel in restricted and nonrestricted areas.

(4) Channeling the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

b. Types of Barriers. Major types of physical barriers are:

(1) Natural rivers, thick vegetation, bays, swamps, and mountains, etc.

(2) Structural fences, walls, doors, gates, roadblocks, vehicle barriers, etc.

c. Clear Zones. An unobstructed area of clear zones will be maintained on both sides of and between permanent physical barriers of restricted and nonrestricted areas. Clear zones are to be 30 feet inside and 20 feet outside.

(1) In certain instances this requirement for clear zones cannot be met. In those instances an exception should be submitted through channels per reference (a).

(2) The Public Works Department will perform maintenance of barriers.

d. Signs. The use of a sign is for posting of boundaries and warnings. The criteria and types of signs for posting boundaries and warnings are:

(1) Restricted areas (including buildings) will be posted at regularly used external points of egress with signs approximately three feet by three feet with proportionate lettering. Signs will read as follows:

15 November 2000

**WARNING
RESTRICTED AREA- KEEP OUT
AUTHORIZED PERSONNEL ONLY**

**AUTHORIZED ENTRY ONTO THIS RESTRICTED AREA
CONSTITUTES CONSENT TO SEARCH OF PERSONNEL
AND PROPERTY UNDER THEIR CONTROL**

INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U. S. C. 797

(2) Perimeter barriers of all restricted areas will be posted with signs measuring approximately 12 inches by 18 inches in size with proportionate lettering. Signs will read as follows:

**WARNING
RESTRICTED AREA
KEEP OUT**

**AUTHORIZED
PERSONNEL ONLY**

(3) Nonrestricted areas will be posted at all points ingress with signs approximately three feet by three feet in size with proportionate lettering. Signs will read as follows:

**WARNING
U.S. NAVY PROPERTY
AUTHORIZED PERSONNEL ONLY**

(4) Perimeters of nonrestricted areas will be posted with signs measuring approximately 11 inches by 12 inches in size with proportionate lettering. Signs will read as follows:

**U.S. GOVERNMENT PROPERTY
NO TRESPASSING**

The interval between signs posted along restricted and nonrestricted area perimeters shall not exceed 200 feet.

(5) The color code for all signs should provide legibility from a distance of at least 100 feet during daylight under normal conditions. The following color codes are recommended for installation/activity and restricted/nonrestricted area perimeter signs:

(a) All words except WARNING will be black.

(b) The word WARNING will be red.

(c) All wording will be on red, white, and blue backgrounds, as appropriate to obtain maximum contrast.

15 November 2000

e. Gates. The gates will be limited to the minimum number required to permit expeditious flow of traffic in and out of the installation or activity. Types of gates are as follows:

(1) Vehicle and pedestrian traffic:

- (a) Gate # 1- King George and Randall Street.
- (b) Gate # 3- Maryland Avenue and Hanover Street.
- (c) Gate # 8- Maryland Route # 450.

(2) Gates used for temporary functions:

- (a) Gate # 2- Pedestrians only.
- (b) Gate # 4- Vehicle and pedestrians.
- (c) Gate # 5- Used on approval from Deputy for Operations.
- (d) Fleet Landing Gate- Used on approval of Deputy for Operations.

(3) The manning of these gates will be by U.S. Marine Guards, U.S. Navy personnel or DOD Police.

(4) The locks for these gates will be rotated per reference (a).

f. Protective Lighting System. Protective lighting provides a means of continuing a degree of security that is maintained during daylight hours. It increases the effectiveness of security forces performing their duties. It has considerable value as a deterrent to thieves and vandals and may make the job of saboteurs or terrorists more difficult. Requirements for protective lighting at an activity will depend on the situation and the areas to be protected. The following should be considered for security lighting:

(1) Provide adequate illumination or compensatory measures to discourage or detect attempts to enter restricted areas and reveal the presence of unauthorized persons within the areas.

(2) Avoid glare lighting which handicaps security force personnel or is objectionable to air, highway, or navigable water traffic or occupants of adjacent properties.

(3) Locate light sources so that illumination is directed toward likely avenues of approach and provides relative darkness for patrol roads, paths, and posts. To minimize exposure to security force personnel, lighting at entry points will be directed at the gate and the guard shall be in the shadows.

(4) It is not the intent of this instruction to prescribe specific protective lighting requirements. Except for minimum standards, the Superintendent must decide what other areas or assets to illuminate and how to do it. The decision must be based upon the following:

15 November 2000

(a) Relative value of items being protected.

(b) Significance of the items being protected in relation to the activity mission and its role in the overall national defense structure.

(c) Availability of security forces to patrol and observe illuminated areas.

(d) Availability of fiscal resources (procurement, installation, and maintenance costs).

(e) Energy conservation.

(5) Protective lighting will be checked daily by the security force during patrol to make sure all light fixtures are operational. Inoperative lights will be recorded and referred to the Watch Commander or Security Officer for corrective action.

(6) Protection of controls and switches for protective lighting will be inside the protected area and locked or guarded at all times. An alternative is to locate controls in a central station for monitoring.

g. Intrusion Detection Systems (IDS). IDS are an essential element of any in-depth physical security program. IDS consist of sensors capable of detecting one or more types of phenomena, signal media, enunciators, and energy sources used for signaling the entry or attempted entry into the area protected by the system. IDS are designed to detect, not prevent, actual or attempted penetrations. IDS are supported by prompt security force response when the system is activated. For IDS to function as security aids the following is necessary:

(1) IDS system will be inspected and tested on a monthly basis. Records will be kept of the test and inspection. The Physical Security Specialist will perform these actions.

(2) The Fire/Police Dispatcher monitors the system on a 24-hour basis. The central location for monitoring is located in the basement of the Public Safety Building, Bldg. # 257. Security personnel on duty will record all openings and closings of IDS. Proper use of the appropriate code words will be used when telephoning the Fire/Police Dispatcher concerning the IDS.

(3) In the event of activation of an IDS, the Fire/Police Dispatcher will dispatch DOD Police patrol units to the IDS zone activated.

(4) Maintenance of IDS, in most cases, is performed by the contractor who installed the system. Maintenance of faulty systems will be reported to the Physical Security Specialist in the Security Department for coordination and proper record keeping.

(5) Offices or buildings with IDS are to locate the IDS panel away from public view and access. The system will be equipped with tamper-proof switches.

(6) The monitor panel located in the Public Safety Building, #257 (basement) will not have public access or viewing. The Fire/Police dispatcher on duty is to prevent any public access to the monitor panel.

15 November 2000

(7) Due to the sensitivity of IDS, the facilities protected and the details of the system will not be covered in this instruction. Information regarding the IDS can be obtained directly from the Physical Security Specialist on a need to know basis only.

h. Security Force Communications. The security force will have its own communications system with direct lines between security headquarters and security elements. An auxiliary power supply (emergency generator) and sufficient equipment to maintain continuous 2-way voice communications among all elements is necessary. Security communications will provide the following:

(1) The means for expeditious transmission of routine and emergency instructions between security headquarters, posts, and patrols.

(2) The integration and coordination of security functions.

(3) The efficient and economical use of security forces.

(4) The expeditious transmission of requests for assistance to outside sources in the event of an emergency beyond the capability of the security force to control.

15 November 2000

SECURITY FORCE

1. Purpose. The security force constitutes one of the most important elements of the installations physical security program. It is one of the Superintendent's most effective and useful tools in a comprehensive integrated physical security program. The security force consists of designated persons specifically organized, trained, and equipped to provide physical security and law enforcement for the command. The USNA security force is composed of the following:
 - a. DOD civilian police.
 - b. U.S. Marine Security Guard Force.
 - c. U.S. Navy Military Police.
 - d. Auxiliary Security Force.
2. Mission. Provide security for USNA/AAC by performing the following:
 - a. Detect, deter, and defeat terrorism.
 - b. Prevent and deter theft and other losses caused by fire damage, accident, trespassing, sabotage, espionage, etc.
 - c. Protect life, property, and the rights of individuals.
 - d. Enforce rules, regulations, and statutes.
3. Organization. The Security Department is organized into the following elements:
 - a. Security Officer
 - (1) Appointed by the Superintendent, USNA.
 - (2) Heads the Security Department. In this capacity, plans, implements, and supervises the entire security program.
 - b. Security Manager
 - (1) Administers the Information and Personnel Security Program for the command.
 - (2) Coordinates background investigations for employees, students, and staff clearances with the Defense Investigative Service.
 - c. Physical Security Specialist
 - (1) Advisor to the Security Officer on physical security matters.
 - (2) Performs physical security inspections/surveys.
 - (3) Chairperson for Loss Prevention Subcommittee.
 - (4) Member of installation Physical Security Review Committee.

15 November 2000

(5) Responsible for coordination of the IDS.

d. Chief of Police

(1) Oversees and administers the day-to-day operation of the Police Department.

(2) Advisor to the Security Officer concerning law enforcement and security matters.

(3) Coordinates and prepares operational plans for special functions involving law enforcement and security (conferences, visiting dignitaries, graduation, etc.). Coordinate and liaison with:

(a) Naval Criminal Investigative Service (NCIS).

(b) Annapolis City Police Department.

(c) Anne Arundel County Police Department.

(d) Maryland State Police.

(4) Prepares and issues Standard Operating Procedures and instructions concerning the operations of the Police Department.

e. Deputy Chief of Police

(1) Oversees the day-to-day operation of the uniform police division.

(2) Reviews all Incident/Complaint Reports and traffic citations.

(3) Determines assignment of personnel to rotating shifts.

(4) Acts as Chief of Police in the absence of the Chief.

f. Detectives

(1) Investigate thefts of \$2500.00 or less or those not accepted by NCIS.

(2) Investigate claims against the government (accidents, theft, personal injury, etc).

(3) Maintain liaison with NCIS.

(4) Perform surveillance on special investigations.

(5) Perform investigations deemed appropriate by the Security Officer.

(6) Appointed as Evidence Custodian and Alternate Custodian.

g. Shift Commanders

(1) Supervise each rotating shift of uniform police.

15 November 2000

(2) Prepare a work schedule for those police assigned to his/her shift.

(3) Advise and assist police personnel concerning law enforcement and security matters during their tour of duty.

(4) Notify NCIS, NADO, or chain of command when serious incidents or information should be passed on immediately.

h. Lead Police Officers (Sergeant)

(1) Acts as Shift Commander in the absence of the Shift Commander.

(2) Supervises and assists police when requested or assigned by the Shift Commander.

(3) Perform law enforcement and security duties including responses to incidents requiring police service.

(4) Performs Field Training Officer duties for his/her shift.

i. Patrolman

(1) Patrol assigned area of responsibility, enforcing regulations, rules and law as appropriate in the performance of his/her duty.

(2) Perform preliminary investigations of incidents (thefts, vandalism, assault, etc.) notifying the shift commander if assistance is required by NCIS, or detectives.

(3) Issue traffic citations, investigate accidents, and testify in U.S. Magistrate's Court on respective cases.

j. Pass and Tag Office

(1) Issue government identification cards to employees and contractors.

(2) Issue decals for vehicles.

(3) Issue contractors temporary passes for vehicles.

4. Weapons and Equipment

a. Weapons Qualification. Each member of the Security Department who is required to carry a weapon will qualify with the 9mm pistol as a prerequisite of employment and will:

(1) Attend quarterly weapons training and qualify annually with his/her assigned weapon.

(2) Attend weapons training for use of the 12-gage shotgun with annual qualification.

(3) Perform 40 hours on-the-job-training with the Doppler Radar before issuing traffic citations for violations of posted speed limits.

15 November 2000

b. Equipment. Equipment for police will be issued on employment (leather belt, holster, handcuffs, badges, jackets, rain coat, etc.).

5. Training

a. Training will be conducted per reference (a).

(1) Phase I (80 hrs) for all new police personnel.

(2) Phase II (40 hrs) in-service training annually.

(3) Roll Call Training.

(4) Specialized training on anti-terrorism, hostage negotiation, bomb threats, etc. This will include mutual training agreements with the Annapolis City Police Department and other Federal, state, and local law enforcement agencies.

6. Use of Sentry/Patrol Dogs

a. The use of sentry/patrol dogs (K-9) will be per reference (j).

(1) The use of drug detector dogs requires a demonstration before the Superintendent. After witnessing the demonstration, the Superintendent may certify the team (dog and handler) as reliable.

(2) The use of dogs (K-9) for drug detection and explosives will be from outside agencies. Support is received from the following:

(a) Anne Arundel County Police Department.

(b) Naval District Washington.

(c) Patuxent River Naval Air Station.

(d) Andrews Air Force Base.

7. Auxiliary Security Force (ASF)

a. Composition. The ASF will be composed of NAVSTA personnel assigned per reference (a).

b. Mission

(1) The ASF will provide security for NAVSTA Annapolis during increased threat conditions, or when directed by the Superintendent and/or Naval Station Commanding Officer.

(2) The ASF will be capable of manning assigned posts/patrols in threat conditions "CHARLIE and DELTA" and sustain that security posture for at least 5 days.

c. Weapons and Equipment

(1) All ASF personnel will be provided with weapons and training for the following weapons:

- (a) 9MM semiautomatic pistol.
- (b) 12-gage shotgun.
- (c) M-16 rifle (at NAVSTA discretion).

(2) Equipment issued to the ASF will consist of the following:

- (a) Web utility belt (pistol).
- (b) Holster for 9MM pistol.
- (c) Canteen and canteen cover.

(d) The wearing of the camouflage uniform is authorized. However, the decision for issuance is by the ASF member's unit. The unit would have the responsibility for ordering the uniforms through the Navy Supply System.

d. Deployment Concept

(1) The size of the ASF is determined based on the size and criticality of the assets to be protected and the number of personnel required to man additional posts to protect the mission of USNA.

(2) ASF members will be assigned to predetermined fixed and mobile posts.

(3) In the event of traffic problems with vehicle travel from NAVSTA to USNA, launch from the NAVSTA Small Craft Division will be used to transport ASF Personnel from the NAVSTA to Hubbard Hall (Dorsey Creek) for unloading. Assembly will be Fire Station #1, located across the street from Hubbard Hall.

e. Training

(1) The NAVSTA Security Officer is responsible for training the ASF.

(2) Personnel assigned to the ASF will be trained in anti-terrorism skills by the Marine Cadre, or by the Mobile Training Teams from the Marine Corps Security Force Battalions.

(3) Following initial training and weapons qualification, ASF members will be assigned security duties twice a month as a means of continued training. Furthermore, the entire ASF will be employed in a quarterly security exercise realistically tailored to prepare members for terrorist and crisis management operations, or other incidents that may occur within their areas of responsibility.

(4) All ASF personnel will be qualified with assigned weapons and will periodically receive training in the use of force per reference (a) chapter 9.

15 November 2000

(5) ASF training schedules are to be established and monitored by the Security Officer, USNA. See paragraph 0909 per reference (a) for information on recording training.

(6) Part 2 of Appendix XII per reference (a) contains minimum training requirements for the ASF.

8. Marine Barracks Annapolis

a. Mission. During THREATCONs "Charlie and Delta" the Marines' primary mission will be to protect the Naval Academy.

b. Deployment Concept

(1) Increased manning at the gates.

(2) Roving perimeter patrols.

(3) Reaction Force.

c. Training. In accordance with reference (i) chapter 9.

15 November 2000

CRISIS MANAGEMENT

1. Situation. The Naval Academy must be prepared to effectively respond to various types of emergencies that may endanger personnel, damage or destroy facilities and equipment, or degrade military capability. Since no two emergencies are alike, preplanning cannot take into account all preparations and contingencies. Therefore, the Superintendent or Deputy for Operations has the right and responsibility to alter this plan in a way to fit the situation at hand.

2. Mission. To provide those security measures and actions necessary to minimize loss of operational capability, resources, and personnel and allow full operational capability to be restored during or as a result of a crisis situation.

3. Execution

a. Concept of Operation

(1) This plan outlines actions to be taken for effective and timely responses in crisis situations.

(2) DOD Police and Fire Department Personnel will be the first responders for most incidents. For any mass casualty incident the Fire Department will set up an on scene incident command center. They will be assisted by local fire and medical teams as provided for under current memorandums of agreement. All gates will be closed to all personnel except emergency response vehicles until entrance of recalled personnel and press can be allowed in an organized manner.

(3) When determined by the Deputy for Operations the Crisis Response Team (CRT) will be assembled. The CRT will consist of a representative from all cost centers, but may be tailored by the Deputy for Operations to only those required to minimize losses and restore operational capability. The Emergency Operations Center (EOC) is located in the public safety building (Bldg. #257). Alumni Hall will house the alternate EOC.

(4) The CRT will assemble ad hoc incident response teams as required based on the skills and capabilities required to minimize damage and restore operational capability.

(5) Appendixes A through E provide preplanned responses to an increase of threat conditions, civil disturbances, hostage situations, sabotage, and bomb threats.

b. Communications. Circuits listed below are used for command and control during a crisis. The Security Officer will ensure that the Naval Station, Naval Medical Clinic (NMCL), Deputy for Operations, Public Works, Dispatch, Marine Barracks, and NADO all have the ability to monitor these circuits via radios available for issue to designated personnel.

(1) Circuit (1), Freq. 139.475 MHz

(2) Circuit (3), Freq. 148.425 MHz

(3) Circuit (4), Freq. 148.950 MHz will be the secondary police circuit.

(4) Circuit (9), Freq. 138.625 MHz NDW Disaster Control Net will be used as a command net to pass reports, etc.

(5) Circuit (10) Freq. 140.625 MHz will be available as a back up fire net or back up Command Circuit.

(6) Other support will be coordinated on existing radio circuits or telephones as available.

(7) The Academy Announcing System will be used to pass gathering instructions and provide guidance for those on Academy grounds. A duress word will be established by the Security Officer annually to indicate if the person operating the system is under duress.

(8) The standing phone numbers to the EOC are:

NMCL	(410) 293-5642
Base Operations	(410) 293-5654
Chaplains/Family Services Center	(410) 293-5655
Public Affairs Office	(410) 293-5656
Public Works Department	(410) 293-5657
Fire/Police	(410) 293-5658

APPENDIX A

THREATCONS

1. Purpose. To prevent terrorist access to the Naval Academy Complex while allowing visitation and operations commensurate with the perceived threat.

2. Threat Assessment

a. The overall Threat Assessment for the United States Naval Academy is low. A low threat is defined as a set of circumstances wherein: "a group with the capability to mount a terrorist act is known to exist; and while such a terrorist group may or may not have a history of prior terrorist acts, there exists no known present intention to undertake a terrorist act."

b. NCIS provides the Threat Assessment for the United States Naval Academy. Reference (r) details USNA's current threat assessment dated 28 September 2000. NCIS will provide additional information relevant to the threat as it becomes available.

c. U.S. Terrorism Highlights

(1) A terrorist attack is most likely to occur as a result of a retaliatory or protest action as a form of revenge or as a publicity stunt. Heightened awareness of the world political situation can help determine how and when to adjust security measures in response to the potential threats. According to the Federal Bureau of Investigation (FBI), approximately 10 terrorist incidents have occurred in the United States since 1990, and since 1982, 10 incidents have taken place in the Washington D.C. area alone. Well-known examples of terrorist acts in the United States include the 1993 bombing of World Trade Center in New York City and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City.

(2) A number of terrorist threats indicate that any Federal facility can become a target. Recently, an anti-government revolutionary group, known as "Revolution 2000" using the return address "Las Vegas, Nevada 89104," sent letters to DOD commands threatening the use of bombs, grenades, mortars, rockets, missiles, and nerve agents to attack politicians, government officials, and facilities.

d. United States Naval Academy Terrorism Concerns. Washington D.C. area possible-terrorist events include the killing of two Central Intelligence Agency (CIA) employees outside CIA headquarters in 1993, a bomb threat to Union Station in 1995, a bomb threat against Bolling Air Force Base in 1996, and a conspiracy to bomb Federal facilities in West Virginia on behalf of an international terrorist organization in 1996. The United States Naval Academy could also become the subject of a bomb threat by a terrorist organization. Likely scenarios could include driving or crashing a vehicle carrying explosives through one of the main gates or penetrating the fenced perimeter or coastline with a small contingent to place explosives at selected facilities. The United States Naval Academy is an open base with over a million visitors a year, which complicates antiterrorism efforts.

2. Collection, Analysis, and Distribution of Terrorist Threat Information

a. Security is an all hands evolution and, as such, suspicious activity must be reported to security as soon as possible. The Security Officer will assess the information and report it to Deputy for Operations and NCIS with recommended action including modifications to THREATCON if appropriate. Information regarding terrorist activity or threat levels received via message traffic or via phone call from Naval District Washington or NCIS will be reported to Base Operations and Deputy for Operations immediately. The USNA Security Officer will contact Annapolis City, Anne Arundel County, and Maryland State Police and inquire about possibly terrorist related activity in the area. NCIS will be contacted and requested to contact other local and Federal law enforcement agencies.

b. Deputy for Operations will determine the best method to disseminate information regarding terrorist activity and an increase in terrorist threat condition. Cost center heads will be notified and e-mail messages to all non-midshipmen will be posted if appropriate. When increase THREATCON is set, signs at the gates indicating the current threat conditions will be posted. The Commandant of Midshipmen will be responsible for disseminating required information to Midshipmen personnel.

c. Navy and Marine Blue Dart Terrorism Threat Warning Message. The Blue Dart message disseminates imminent terrorism threat warnings and is disseminated by the Navy Anti-Terrorism Alert Center (NAVATAC) when intelligence indicates that a specific, imminent, and credible terrorist threat exists. In addition, any Commander within the DON may send a Blue Dart message. Blue Dart messages must meet the following threat definitions:

(1) Specific. A particular location or organization must be identified.

(2) Imminent. The event is to occur within 72 hours.

(3) Credible. Corroborated information or information received from a source of assessed reliability. The Blue Dart message will be received by the Message Branch and will be immediately hand delivered to the NADO. The NADO will acknowledge the message by immediate message and notify Base Operations and the Security Officer. After normal duty hours NCTS Washington will notify the USNA emergency dispatcher, who will then notify required personnel utilizing the emergency notification matrix.

3. General. Terrorist threat conditions and their associated suggested security measures are established as follows: The decision to arrive at a particular THREATCON should be based on multiple factors that may include threat, target vulnerability, criticality of assets, security resource availability, international relations, and planned U.S. Government actions that could trigger a terrorist response.

a. THREATCON NORMAL. A general threat of possible terrorist activity exists, but warrants only a routine security posture.

b. THREATCON ALPHA. A general threat of possible terrorist activity, the nature and extend 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 higher THREATCONS resulting from

15 November 2000

intelligence received or as a deterrent. The measures in that 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 Naval installations, activities, or facilities; and be alert for abandoned parcels or suitcases or any unusual activity.

(a) USNA will send out a home security checklist to each active duty service member and will place periodic e-mail and Plan of the Day announcements to increase security awareness and provide security measures for personal protection from terrorist attack.

(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, available at all times. Keep key personnel who may be needed to implement security plans on call. Instruct all cost centers to verify recall lists. All cost center heads will verify recall lists are up to date.

(3) Measure 3. Secure buildings, rooms, and storage areas not in regular use. Each cost center head will conduct building security checks at the close of business each day to ensure buildings, rooms, and storage areas are locked. A log will be used to identify who is in the building after it has been secured.

(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 only 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 15). DOD police will conduct external door checks of key assets on the Academy. The Duty Officer will be contacted if the building is found unsecured.

(b) At the beginning and end of each workday and at other regular and frequent intervals, inspect for suspicious activity or packages in the interior and exterior of buildings in regular use. (Measure 16).

(c) Check all deliveries to messes, clubs, etc. (Advise dependents to check all home deliveries). (Measure 18). Persons receiving shipment will verify delivery against packing documents and report suspicious deliveries to the Security Officer.

(d) As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve

A-3

Enclosure (1)
Appendix (A)

For Official Use Only

deterrence and defense and build confidence among staff and dependents. (Measure 19). Minimum manning of DOD police will be at least three personnel. Minimum manning of patrol force will not be waived during THREATCON ALPHA or above.

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

(8) Measure 8. As appropriate, review and implement security measures for high-risk personnel; e.g., direct use of inconspicuous body armor. Coordinate with Superintendent's Office for desired level of personal security requirements.

(9) Measure 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(10) Measure 10. Spare.

c. THREATCON BRAVO. An increased and more predictable threat of terrorist activity exists. The measures of this threat condition must be capable of being maintained for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

(1) Measure 11. Repeat Measure 1 and warn involved personnel of any other form of attack to be used by terrorists.

(2) Measure 12. Keep all personnel involved in implementing anti-terrorist contingency plans on call. Run operation test of cost center recall lists.

(3) Measure 13. Check plans for implementation of the measures contained in the next higher THREATCON. Barricades will be placed near gates to speed up implementation of THREATCON CHARLIE measures.

(4) Measure 14. Where possible, cars and objects such 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. Post signs, publish e-mail, and local notices indicating no parking within 80 feet of key buildings or in parking spaces marked with a yellow triangle.

(5) Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use. Daily checks of all buildings within a work center will be checked. DOD Police will continue building checks as directed.

(6) Measure 16. At the beginning and end of each workday and at other regular and frequent intervals, inspect for suspicious activity or package on the interior and exterior of buildings in regular use. Duty officers will implement periodic building checks within each workday.

(7) Measure 17. Examine all mail for letter or parcel bombs. All personnel handling mail will receive a refresher briefing on detection of suspicious packages. The hospital will be contacted to determine the availability of a portable x-ray machine.

(8) Measure 18. Check all deliveries to messes, clubs, etc. (Advise dependents to check all home deliveries). Commercial deliveries will be routed to

15 November 2000

Perry Center for inspection. A special color-coded pass with a time reference will be issued to vehicles after inspection is completed. Vehicles will have no more than 30 minutes to enter the Academy upon completion of inspection.

(9) Measure 19. 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. One or more Marine patrols will be activated to patrol the perimeter of the Naval Academy.

(10) Measure 20. Make staff and dependents aware of the general situation to stop rumors and prevent unnecessary alarm. Additional notification will be passed by e-mail to all staff and faculty personnel. Signs will be posted at each gate indicating the current THREATCON.

(11) Measure 21. At an early stage, inform members of local security committees of any action being taken and why. A special meeting of the Physical Security Review Board will be called.

(12) Measure 22. Upon entry of visitors to the command, physically inspect them and a percentage of their suitcases, parcels, and other containers. Visitors will be routed to gate one where Magnetron Gates will be used to search personnel.

(13) Measure 23. Wherever possible, operate random patrols to check vehicles, people, and buildings.

(14) Measure 24. 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 cars.

(15) Measure 25. Implement additional security measures for high-risk personnel, as appropriate. The Executive Assistant will be contacted to coordinate additional security measures for the Superintendent.

(16) Measure 26. Brief personnel who may augment guard force on use of deadly force and/or rules of engagement. The ASF will receive use of force instruction in accordance with existing USNA guidance.

(17) Measure 27. As appropriate, consult local authorities on the threat and mutual anti-terrorism measures.

(18) Measure 28. Provide increased security surveillance of waterfront areas including wharfs, piers, caissons, critical communication facilities/assets, etc.

(19) Measure 29. Spares.

(a) All visitors will enter the USNA via gate 1 and sign in. Access to Perry Center will be controlled by closing the Annapolis Street gate and placing a 24-hour guard at the King George Street gate.

(b) Key personnel to include the NMCL Commanding Officer, NAVSTA CO, Deputy for Operations, Public Works Officer, Base Operations and Naval Academy Duty Officers will carry a radio tuned to the Disaster Coordination Net (Channel 9).

A-5

Enclosure (1)
Appendix (A)

For Official Use Only

15 November 2000

d. THREATCON CHARLIE. When an incident occurs or when intelligence is received indicating that some form of terrorist action against installations 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. Duty officers will be birthed in Bancroft or Ricketts Hall.

(3) Measure 32. Limit access points to an absolute minimum. Routine access will be via Gate 8. General visitation will be secured.

(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. Employees will park at the Navy-Marine Corps Memorial Stadium and walk or take a bus to their place of employment. Handicapped employees will be given first priority for buses.

(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, dry docks, etc. The EOC will be stood up.

(8) Measure 37. Protect all designated vulnerable points (VPs) and give special attention to VPs outside Naval installations and activities. Place a guard at the water treatment plant in Perry Circle during unoccupied periods.

(9) Measure 38. Erect barriers and obstacles to control traffic flow. Barriers will be set up per enclosure (1) of this appendix.

(10) Measure 39. Consult local authorities about closing public (and Naval) roads and facilities that might make sites more vulnerable to terrorist attacks.

(11) Measure 40. Spare.

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

(1) Measure 41. Continue or introduce all measure listed for THREATCON BRAVO and CHARLIE.

15 November 2000

(2) Measure 42. Augment guard and/or police forces as necessary. Marines will be used as the primary security force for the Naval Academy. Other personnel will be assigned security duties as necessary by the Deputy for Operations or the Commandant of Midshipmen.

(3) Measure 43. Identify all vehicles already on the installation within operational or mission support areas.

(4) Measure 44. Search all vehicles and contents entering the complex or installation.

(5) Measure 45. Control all base access points and implement positive identification of all personnel. Employees will park at the Stadium and ride the assigned busses to the Naval Academy. Routine visitors will not be allowed to enter the Academy.

(6) Measure 46. Search all suitcases, briefcases, packages, etc., brought into the installation or command.

(7) Measure 47. Control access to all areas under the jurisdiction of the Naval installation or command concerned.

(8) Measure 48. Make frequent checks of the exterior of buildings and parking areas.

(9) Measure 49. Minimize all administrative journeys and visits.

(10) Measure 50. Consult local authorities about closing public (and Naval) roads and facilities that might make sites vulnerable to terrorist attack.

(11) Measure 51. 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.). Place a 24-hour guard at the Water Treatment plant in Perry Circle.

3. Threat Assessment Guidelines

a. General Guidelines. The following general guidelines provide for uniform implementation of security alert conditions. Threat levels are determined by an assessment of the situation using the following six terrorist threat factors:

(1) Existence. A terrorist group is present, assessed to be 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, stated or assessed intent to conduct such activity.

(4) History. Demonstrated terrorist activity over time.

15 November 2000

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

(6) Security Environment. The internal policy 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, 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. 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 interests.

15 November 2000

APPENDIX A
ENCLOSURE 1Barricade Plan

Location	THREATCON			
	ALPHA	BRAVO	CHARLIE	DELTA
Gate 1	No Barricade	(4) Pre-Positioned Jersey Bouncers	(4) Jersey Bouncers	(4) Jersey Bouncers
Gate 2	Double Locked Gate	(1) Jersey Bouncer	(1) Jersey Bouncer	(1) Jersey Bouncer
Gate 3	No Barricade	No Barricade	Van	Van
Gate 4	Locked and Chained	(2) Jersey Bouncers	(2) Jersey Bouncers	(2) Jersey Bouncers
Gate 5	Locked and Chained	(1) Jersey Bouncer	(1) Jersey Bouncer	(1) Jersey Bouncer
Gate 7	Locked and Chained	Double Locked Gate	Double Locked Gate	Double Locked Gate
Gate 8	No Barricade	(4) Pre-Positioned Jersey Bouncers	(4) Jersey Bouncers-Serpentine	(4) Jersey Bouncers-Serpentine
Gate 10	Locked and Chained	Locked and Chained	Locked and Chained	Locked and Chained
BG & E Gate	Locked and Chained	(2) Jersey Bouncers	(2) Jersey Bouncers	(2) Jersey Bouncers
King George Street Gate	No Barricade	(2) Jersey Bouncers-Serpentine	(2) Jersey Bouncers-Serpentine	(2) Jersey Bouncers-Serpentine
Annapolis Street Gate	Locked and Chained	(2) Jersey Bouncers	(2) Jersey Bouncers	(2) Jersey Bouncers
Perry Circle Road	No Barricade	(2) Pre-Positioned Jersey Bouncers	(2) Jersey Bouncers-Serpentine	(2) Jersey Bouncers-Serpentine
Sellers Road	No Barricade	(2) Pre-Positioned Jersey Bouncers	(3) Jersey Bouncers-Serpentine	(3) Jersey Bouncers-Serpentine
Brownson Road	No Barricade	No Barricade	Stake Bed Truck	Stake Bed Truck
Decateur and Parker	No Barricade	No Barricade	Stake Bed Truck	Stake Bed Truck
Hill Bridge	No Barricade	No Barricade	Dump Truck	Dump Truck
Cooper Road North	No Barricade	No Barricade	Locked Swing Gate	Locked Swing Gate
Cooper Road South	No Barricade	No Barricade	Locked Swing Gate	Locked Swing Gate
Holloway Road North	No Barricade	(3) Pre-Positioned Jersey Bouncers	(3) Jersey Bouncers	(3) Jersey Bouncers
Holloway Road South	No Barricade	(2) Pre-Positioned Jersey Bouncers	(2) Jersey Bouncers	(2) Jersey Bouncers

A-9

Enclosure (1)
Appendix (A)

For Official Use Only

15 November 2000

APPENDIX B

CIVIL DISTURBANCE

1. Situation. The Naval Academy could possibly become involved in planned or spontaneous demonstrations. To avoid entirely, or minimize damage resulting from such incidents, security measures will be adopted as outlined here.
2. General. Any disturbance experienced in the Naval Academy area would arrive from one of two directions. The first direction would be from the City of Annapolis. The second possible direction would be from the north using the U.S. Naval Academy Bridge (MD Route # 450) to Gate # 8. Side activity could occur at the entrance to the NAVSTA or USNA, North Severn, Annapolis, MD. The increased security plan prescribed here provides for increased surveillance inside the Naval Academy perimeter and adjacent housing areas using security patrols in sectors to enable early detection of possible destruction of government property.
3. Execution
 - a. Patrol Sector
 - (1) Sector A, beginning at Fleet Landing along the fence inside the Halsey Field House parking lot and along the rear of Porter Road to Scales Road.
 - (2) Sector B, from Scales Road, along the wall behind the Chapel and Administration Building past Gate # 3, down Nulton Road behind the O&F Club to Balch Road.
 - (3) Sector C, will be Balch Road, inside the wall along North Boundary Road, behind Upshur Road quarters to Dorsey Creek.
 - (4) Sector D, inside the fence behind Lawrence Field from Dorsey Creek, around Halligan Hall to Gate # 8.
 - (5) Sector E, from Gate # 8, inside the fence to the Naval Academy Bridge.
 - (6) Sector F, Water Front areas to include, Turner Joy Road to Santee Basin along Sims Road, McNair Road, Ramsey Road, and Hospital Point Area.
 - (7) Sector G, Perry Center Shops Complex, Laundry, Water Treatment Plant, Power Plant, Arundel Estates Housing Area, Badger and Sellers Road Housing Area.
 - b. Security Alert Conditions. The following alert conditions will establish the degree of security that will be implemented during various levels of alert conditions. The alert conditions will be set by Deputy for Operations, or in his/her absence, the Security Officer, USNA.
 - (1) Condition V will be normal security and working conditions. All personnel will be alert to conditions of civil unrest within the area. Any incidents that are observed will be reported to their supervisors.
 - (2) Condition IV will be based on confirmation of anti-military activities or other demonstration activities that could affect the Annapolis Area Complex. The following organizations will be alerted for increased security requirements:

B-1

Enclosure (1)
Appendix (B)

For Official Use Only

15 November 2000

(a) Marine Barracks, NAVSTA, Fire Department, USNA Police, Naval Station Police, CBU-403, and Bancroft Hall.

(b) USNA Police will initiate continuous patrols of the Naval Academy.

(c) Security patrol equipment will be made immediately available for issue from the Security Command Post.

(d) Five vehicles from Public Works Transportation will be delivered to the Security Command Post, Building # 257.

(e) The Public Affairs Officer will be alerted and briefed as to the present conditions.

(3) Condition III will be the result of information or occurring disorder leading to the possibility of large demonstrations or riot activities occurring in Anne Arundel County and the Annapolis Area Complex or riot activities in the City of Annapolis, MD.

(a) Mutual aid assistance will continue; however, only the Deputy for Operations, Security Officer, or NADO may authorize fire fighting equipment or ambulances to respond to emergency request from civil authorities.

(b) Civil authorities will be requested to provide police protection for fire fighting personnel and equipment.

(c) The Security Command Post will report all action taken on request for emergency response and equipment to the Commandant Naval District Washington (NDW), D.C.

(d) NADO will be assigned to the Security Command Post.

(e) ASF will be activated with 15 members responding to the Security Command Post for briefing and posting by the Security Officer, USNA.

(f) Two members of the ASF will be posted in each of the five sectors with portable radios (walkie-talkie). Five members will be held in reserve at the Security Command Post.

(g) The additional security patrols and sentries will be placed on standby. The remainder of the ASF will be on NAVSTA premises and should be ready to embark for the USNA on short notice.

(h) NAVSTA Boat Crews (Small Craft Division) will be alerted and ready to transport ASF personnel from the NAVSTA to Hubbard Hall on a 20-minute notice.

(i) Begin Harbor Patrol with one Yard Patrol (YP), using Harbor Control frequency, manned by Sailing Center personnel.

(j) Liberty suspended. All off-duty NAVSTA and Naval Academy Police personnel recalled.

(k) General visiting suspended at the Naval Academy.

B-2

Enclosure (1)
Appendix (B)

For Official Use Only

15 November 2000

- (l) Public Affairs Officer on standby.
- (m) Marine Barracks personnel mustered in Marine Barracks.
- (n) Alternate Command Post established at Firehouse # 1, USNA.

(4) Condition II will be implemented on confirmed reports of uncontrolled riotous activity within the City of Annapolis.

(a) Activate ASF.

(b) Transport Marine Security Force to Hubbard Hall via ground transportation, if the Naval Academy Bridge is closed, the Marines will be transported via boat to Hubbard Hall.

(c) Brief and issue equipment to security patrols at Security Command Post (Building # 257).

(d) The NDW Disaster Control Circuit between USNA and NDW control center will be activated.

(e) NADO will alert other commands within the Annapolis Area Complex.

(f) NMCL will be placed on alert if deemed necessary by the Deputy for Operations or his/her representative.

(g) All gates or those which may be affected by the riotous activity will be closed as the situation dictates.

(h) Alert and assemble midshipmen forces, Company Officer-in-Charge, Midshipman first class in charge of each platoon.

(i) The Public Affairs Officer will establish a command information center that will function on a 24-hour basis.

(j) The Marine Barracks will issue weapons with additional ammunition and deploy to a central position which will facilitate rapid deployment to any endangered location of the Annapolis Area Complex.

(5) Condition I will be disorderly conditions out of control in the City of Annapolis or vicinity and likely to approach the Naval Academy.

(a) Maximum security measures implemented to include use of DOD Police, Marine Security Guards, ASF, etc. Weapons of military patrols will be loaded.

(b) Close contact will be maintained with other area commands.

(c) Fire Department equipment will be dispatched as necessary.

(d) Midshipmen forces will be deployed as necessary to assist in preventing forced entry into the Naval Academy property.

15 November 2000

4. Responsibilities

a. Deputy for Operations, USNA is responsible to the Superintendent for the execution of this instruction.

b. Security Officer, USNA will:

(1) Increase security conditions as required.

(2) Maintain liaison with city, county, state, and Federal agencies.

(3) Upon direction of Superintendent or Deputy for Operations, set security alert conditions appropriate for immediate situations.

(4) Notify Superintendent; Commandant of Midshipmen; Deputy for Operations; CO, NAVSTA; CO, Marine Barracks; NADO; NCIS; and OIC, CBU-403 of situation and keep them informed.

(5) Establish Security Command Post in USNA Police Headquarters (Building # 257) and take control of security forces.

(6) Recall Chief of Police and Fire Chief as required.

(7) Make sure all personnel involved with civil disturbance operations receive a copy of this instruction.

(8) Issue all portable communications equipment as necessary to insure adequate command and control of security patrols.

c. NADO will:

(1) Take station in Security Command Post on Condition III.

(2) Alert and keep posted area commands and certain key personnel concerning the Naval Academy existing situations as follows:

(a) NDW Duty Officer.

(b) Navy Department Duty Captain.

(c) CNO Duty Captain.

(d) CO NMCL.

(e) Ships present at USNA.

(f) Department Heads (if required).

d. Commandant of Midshipman, USNA will:

(1) Notify appropriate civil authorities of expiration of liberty for midshipmen and request assistance in directing their immediate return to the USNA.

(2) Activate Bancroft Hall Command Post when required by alert conditions.

15 November 2000

(3) Deploy midshipmen if necessary.

e. CO, NAVSTA will:

(1) Provide security for NAVSTA, Annapolis, MD.

(2) Provide ASF for deployment to USNA.

(3) Provide boat transportation for Marines and ASF between NAVSTA and USNA.

(4) Activate YPs, for seawall and harbor area. Control Net 2716 KC.

(5) Provide arms and ammunition for ASF.

f. CO, NMCL USNA will provide medical assistance as required.

g. Commanding Officers of Ships Present, Annapolis Area will:

(1) Cancel liberty and recall personnel when readiness condition III is set.

(2) Maintain close liaison with NADO at Security Command Post.

(3) Provide assistance if requested, such as, landing party, backup communications, and fire fighting parties.

APPENDIX C

HOSTAGE SITUATION

1. Purpose. Establish policy and procedures for response and handling of captor/hostage situations.
2. General. A terrorist group or individual(s) not associated with a terrorist group may undertake the seizure of specific hostage(s) for ransom, media attention, coercion, or political bargaining purposes. An armed attack may be used to seize critical assets or personnel to use the assets or personnel as leverage to bargain for publicity, escape, ransom, and political advantage. This crisis incident could rapidly escalate to include a government crisis management overview at the highest levels.
3. Mission. Control the crisis situation using proper procedures to resolve the situation and prevent the incident from expanding.
4. Execution
 - a. Notification of incident
 - (1) Upon notification of a barricaded captor/hostage situation within the Annapolis Area Complex, the following measures will be taken:
 - (a) Police officer receiving such information will immediately notify the Shift Commander (senior police officer on duty), NCIS, and the USNA Security Officer of the situation. If after duty hours, the Shift Commander will notify the NADO.
 - (b) The police officer and shift commander will respond to the scene to conduct a preliminary investigation and determine the nature of the situation. At this stage, discretion is mandatory when approaching a possible crisis management scene. Police sirens will not be used. No firearms are to be used at this point except in a self-defense or life-saving situation.
 - (c) Having verified that a crisis management situation exists, the senior police officer on the scene will report the circumstances to the Police/Fire Dispatcher, informing him/her that a CODE 10-33 is established to indicate a crisis management situation.
 - (d) Fire/Police Dispatcher will notify the following personnel
 - 1 Deputy for Operations.
 - 2 Base Operations Officer.
 - 3 SJA.
 - 4 NCIS (will furnish hostage negotiator and team).
 - 5 Duty Officer for Marine Barracks, NAVSTA.
 - 6 Fire Department, USNA.

15 November 2000

7 Public Works Department, USNA.

8 Alert NMCL (Possible need of ambulance and psychiatrist).

9 Officer Personnel, USNA.

5. Responsibilities

a. Security Officer, USNA will:

(1) Assume responsibility as the on-scene-commander until the arrival of Deputy for Operations. Thereafter, when relieved, assist Deputy for Operations as required.

(2) Direct the establishment of a cordoned perimeter to seal off the immediate area.

(3) Institute the evacuation procedures for all personnel from buildings/offices in the immediate area and verify identities of all officials entering the area. Law enforcement personnel in civilian attire (NCIS, FBI, USNA Detectives, etc.) will display proper badges on outer clothing.

(4) Alert Communications Center to activate the Crisis Response Center.

(5) Make sure a complete log of all telephone calls and radio traffic is maintained.

(6) Contain the scene and keep the area as calm as possible. Upon arrival, transfer the on-the-scene responsibility for investigation, intelligence collection, and hostage negotiation to NCIS. However, the USNA police will continue to provide containment and remain on duty to be used as needed.

(7) Coordinate with local law enforcement agencies if assistance is requested and control of vehicular traffic and pedestrians.

(8) Establish required security perimeters to contain hostage situation.

(9) Arrange for relief of security forces if negotiations extend for a long period of time. Arrange for meals for those required to remain on station.

(10) At the conclusion of the hostage situation, compile records and data to assist NCIS personnel in preparing a final report.

b. Deputy for Operations, USNA will:

(1) Notify the Superintendent, USNA to advise him/her of the situation (after hours) the NADO will inform Deputy for Operations and take instruction from him/her.

(2) Will establish the Crisis Response Center.

(3) Assume responsibility as the on-scene-commander.

(4) Use the services of the Security Officer as Assistant on-scene-commander.

(5) Submit OPREP-3 reports per reference (k).

(6) Make sure all participants are instructed that no personnel except the Public Affairs Officer (PAO) will provide any information to the press.

(7) Keep the Superintendent continually informed.

c. NCIS will:

(1) Provide professional advice to the Superintendent and the on-scene-commander of the operation.

(2) Maintain investigative responsibility per jurisdiction set forth in Department of Navy directives. Investigation in the barricaded/hostage context means in-progress investigation and collection of evidence by all available means.

(3) Interview any hostages released. Also interview any personnel when relieved from the inner perimeter for both evidentiary and intelligence purposes. Appropriately process the crime scene after completion of the incident.

(4) Collect intelligence, with assistance from the security force, concerning the physical environment in which the barricaded captor/hostage situation has taken place, such as floor plans, building layouts, available means of communication within the locale and other information of value to the on-scene-commander.

(5) Collect intelligence information concerning the background of both captor(s) and hostage(s) as appropriate.

(6) Provide hostage negotiator and coordinate their activities. If possible, special agents trained in hostage negotiations will be used.

(7) If required, provide liaison between the command and other law enforcement agencies, particularly the FBI, for the purpose of collecting data and obtaining assistance in the form of equipment and/or personnel to meet the situation at hand. Jurisdiction questions will be decided upon by mutual consent.

d. CO, Marine Barracks, Annapolis, MD will:

(1) On order, deploy the Security Alert Teams to establish an outer perimeter around the captor/hostage site as directed by the on-scene-commander.

(2) Place the Marine Barracks on alert. Muster all available Marines to establish a Guard Reaction Force.

(3) On order, deploy the Guard Reaction Force to the captor/hostage area as directed by the on-scene-commander.

(4) Be prepared to recall Marines from a liberty status.

15 November 2000

(5) CO, Marine Barracks, or his/her designated representative will exercise tactical control and deploy Marines as directed by the on-scene-commander.

(6) CO, Marine Barracks will make sure personnel in his/her command are trained to correctly react in captor/hostage situation.

e. Public Works Officer, USNA will:

(1) Provide emergency lighting systems and provide sufficient personnel to operate the system in the event the area needs to be illuminated.

(2) Provide a portable public address system with adequate back-up units to the Command Post.

(3) Provide an electrician who is familiar with electrical wiring and fixtures of the hostage site.

(4) Provide a representative from the telephone company to set up additional phone lines at the Command Center and disable all but one phone line leading into the hostage site.

(5) Provide a qualified locksmith with tools and equipment for contingency use as required.

(6) Provide a transportation coordinator to the Command Post and extra vehicles as required by the on-scene-commander.

(7) Provide personnel familiar with plumbing, heating and air conditioning systems as required.

(8) Provide requested equipment under control of the Public Works that the on-scene-commander determines may be necessary for the situation.

(9) Provide plats (maps) and building prints of the effected area to the on-scene-commander and the Command Center (Bldg. # 121).

f. CO, NMCL, USNA will:

(1) Arrange for a psychiatrist to assist in negotiations if requested.

(2) Render medical assistance to personnel at the crisis management scene as requested.

g. PAO, USNA will:

(1) Coordinate all aspects of relations with news media under the direction of the on-scene-commander.

(2) Prepare news releases that will be cleared by the on-scene-commander.

(3) He/She will make sure that all news media personnel are restricted in movement. They will not be permitted in the Command Post but kept in a designated press area and given information as cleared by the on-scene-commander.

15 November 2000

(4) Request the cooperation of the news media to avoid speculation as to the motives and intentions of the captors or hostages directly. Cooperation of the press in these matters is essential.

C-5

For Official Use Only

Enclosure (1)
Appendix (C)

APPENDIX D

SABOTAGE

1. Purpose. Establish procedures and methods for preventing and recognizing sabotage. To employ effective countermeasures against the threat of sabotage.
2. General. The willful obstruction or interference with defense activities during wartime are prosecuted by 18 U.S.C. 2151-56. During peacetime "sabotage" is referred to as "wrongful destruction." It includes such things as willfully injuring, interfering with or obstructing the United States or any associate nation in their preparation for or carrying on of defense activities.
3. Mission. Protect life, government assets, and restore mission capability and normal operations as soon as possible.
4. Execution
 - a. Initial response. The person discovering the sabotage or wrongful destruction that significantly impairs mission capability will take action within their capability to limit damage and restore mission capability.
 - b. Initial response by fire or public persons will be designed to limit further injuries and preserve the crime scene for investigation.
 - (1) The senior police officer present will assume the role of on scene commander until relieved as directed by the Deputy for Operations or Security Officer. The on-scene-commander will direct the notification of NADO (if after normal working hours), Deputy for Operations, Base Operations, Security, PAO, NCIS, and the duty department head, as applicable.
 - (2) Establish a perimeter with DOD forces and the Marine Reaction Team if necessary.
 - (3) When relieved as the on-scene-commander provide support as directed.
 - c. The on-scene-commander will have to determine criticality of the system imparted and weigh the maintenance of mission capability against the requirement to preserve the crime scene. If at all possible the crime scene must be preserved.
 - (1) Make reports including OPREPs and unit SITREPs as the situation and press interests dictate.
 - (2) Establish a local command center.
 - (3) Establish access control to the scene and to the command center.
 - (4) Advise Deputy for Operations on the necessity of manning the Crisis Response Center.

APPENDIX E

BOMB THREATS

1. Purpose. To establish policy and procedures for response and handling of bomb threats to buildings and facilities of the Naval Academy.

2. General. Since 1972, more than 400 DOD persons have been killed by terrorists and 67 percent of all terrorist attacks are from bombs. While the number of bomb threats received by military organizations is small, a few are still received. Therefore, everyone must be aware of the correct procedures for handling such disruptive and potentially serious events. Statistically, less than 1 percent of all bomb threats received actually involve a real explosive device.

3. Mission. Protection of life, government assets, and restoration of normal operations as rapidly as possible.

4. Execution

a. Initial Response by Personnel Receiving the Bomb Threat

(1) All personnel, especially those answering department/division telephones or telephone switchboards, will be instructed by supervisors on the sequence of actions to be followed in the event of a bomb threat. Supervisors will ensure that personnel are provided with (enclosure 2), Department of the Navy Telephonic Threat Complaint Form (OPNAV 5527/8). This form will be used for reference and recording of information. The recommended response sequence is:

(a) Record the time of call, telephone extension called, sex, and voice characteristics of the caller.

(b) If possible, record every word spoken by the caller.

(c) If the caller does not initially indicate the location of the bomb, type of bomb, and time of possible detonation, the person receiving the call should ask for this information from the caller.

(d) Pay particular attention to any strange or peculiar background noises such as machinery, background music, and other noises which might give even a remote clue as to the place from which the call is being made.

(e) Attempt to engage the caller in conversation long enough to obtain elements of identity and as much information regarding the bomb and the perpetrator as possible.

(2) Immediately contact the Fire/Police Dispatcher at extension 3-3333. Promptly report the threat to your supervisor or someone in authority.

(3) Evacuate the building by the quickest method available including the use of the fire alarm.

15 November 2000

b. Response by Fire/Police Dispatcher

(1) If the dispatcher receives the bomb threat directly, they will follow procedures outlined in para a, 1(a) thru 1(e).

(2) If dispatcher receives a report of a bomb threat, the dispatcher will:

(a) Alert and dispatch DoD Police to scene of bomb threat.

(b) Notify all personnel concerned using the Security Department Emergency Notification Matrix.

(c) Remind responding units to secure radio communications prior to entering the area of the reported bomb.

(d) Tell the individual who actually received the threat to meet the on-scene-commander at the scene immediately.

c. Response by Deputy for Operations. Upon receipt of a bomb threat against Naval Academy buildings/facilities, the Deputy for Operations or, after normal working hours, and on weekends and holidays, the NADO will:

(1) Assess the validity of the threat.

(a) For bomb threats considered to be authentic, notify the Immediate Chain of Command.

(b) Notify the Chief of Naval Operations Duty Captain by voice WITHIN 5 MINUTES USING REFERENCE (a) OPREP-3 FORMAT.

(c) Notify the Commandant, NDW, DC (Operations/Duty Officer).

(d) Submit an initial Special Incident Report (OPREP-3 NAVY BLUE) message (within 20 minutes) for incidents involving an actual bomb or Unit Situation Reports (UNIT SITREP) for situations involving bomb hoaxes. Reference (a) provides detailed guidance on voice and message OPREP reporting. A copy of reference (a) is maintained in the NADO briefcase along with formatted message guides for use by the Deputy for Operations and/or the NADO.

(e) Activate the Emergency Response Center if deemed appropriate or in any case if an explosion occurs.

d. Response by Security Officer/NADO

(1) Make assessment as to the legitimacy of the threat and evacuate the building. A search of the building should be conducted to ensure all occupants have left the building if possible without placing the search party in imminent danger.

(2) Ensure all occupants of the building are accounted for.

(3) Act as on-scene-commander, set up a perimeter using DOD Police, the Marine Reaction or ASF, military personnel, and civilian employee volunteers as available.

15 November 2000

(4) Contact local law enforcement agencies to determine availability of dogs.

(5) Notify the NMCL during normal working hours. In case the threat proves to be real and immediate, initiate the Disaster Control Plan and call the 24-hour emergency extensions.

(6) Contact the Resident Agent of the NCIS.

(7) If a possible explosive device is found, request assistance from Explosive Ordnance Detachment (EOD) at Fort Meade. If Fort Meade EOD personnel are occupied contact Quantico for available EOD forces. Dogs may be used to help identify explosive materials and are available from local law enforcement agencies and Patuxent River Air Station.

(8) If an explosion occurs, account for response personnel, order electrical power and water secured to the scene and other actions as required to minimize losses and restore operational capability. A landing zone may need to be established. Ensure medical, public works, chaplain and a logistics rep arrive at the on-scene-command center.

e. Bomb Search. If time permits, all persons will search their immediate surroundings, files, and personal desks before evacuating the building.

(1) If a time of detonation is indicated, no one should go near the building within plus or minus 30 minutes of that time.

(2) Personnel who reside or work within the area, accompanied by a security officer, will comprise the primary search teams. The search pattern for a building is from outside to inside, bottom to top. In searching a building without a clue as to where the bomb has been planted, the search party will split into pairs and begin the search from outside inward toward the building. Once the outer perimeter is determined to be clear, the search party will enter the building through the entrance searching at the street level into the center of the building. From there, the search will progress downward through the stairwells and elevators to the bottom floor. If sufficient personnel are available, part of the team may be directed to simultaneously proceed upward from the street floor.

(3) If some clue was given as to the possible location of the bomb, the search should originate at the point or area indicated and spread outward to the outer limits of the building. From there, the search may be directed upward and/or downward depending on the number of personnel available in the search party and the origin of the search.

(4) Bomb or Suspicious Object Found. If a suspicious object is found in the course of a search, do not touch it. The on-scene-commander will call for an immediate evacuation of the area and have it cordoned off allowing for a liberal safety zone. Notify EOD at this time. The on-scene-commander will make sure the area remains vacant until a member of the EOD Team has cleared the area for access. When the on-scene-commander has determined the area to be clear, they will recommend to the appropriate commander that the building be re-entered and normal work resumed.

15 November 2000

5. Responsibilities

a. Cost-center Heads

(1) Department/Cost Center Heads will designate and train personnel within their buildings/facilities to act as search teams. Search teams members; do not need to be experts, just aware of what is normally in the building/areas. The search team escorted by a security officer will mark areas and spaces that have been searched using tape or other markings so other teams will know the area has been searched. If suspicious packages or items are found, advise the on-scene-commander.

(2) Have a written evacuation plan posted in conspicuous areas of the buildings, and ensure that all occupants of the building are aware of the plan.

(3) Have designated evacuation routes marked, indicating they are evacuation routes.

(4) Have emergency evacuation signal. Ensure all occupants are aware of the signal.

(5) Have designated areas outside and a safe distance from the building being evacuated where supervisors can account for their assigned personnel.

(6) Train occupants of the building in their responsibilities prior to evacuating the building; i.e., close safes, file cabinets, or other areas that may contain classified or sensitive information or items. Report unusual or suspicious packages within their work area.

(7) Have a predetermined signal that it is safe to return to building.

(8) Recommend evacuation drills and search team drills.

b. Public Works Officer. Have personnel on standby to

(1) Provide a portable public address system to the on-scene-commander.

(2) Provide equipment and personnel under the control of the Public Works Department as requested by the on-scene-commander including emergency lighting, heavy equipment, etc.

c. Public Affairs Officer. The PAO will coordinate all aspects of relations with news media under the direction of the Deputy for Operations and the on-scene-commander.

d. DOD Police

(1) Respond to scene of bomb threat.

(2) Ensure Radios (RF) are turned off prior to arrival on scene.

(3) The first officer on the scene will make contact with the person who notified security of the bomb threat and evaluate information received from contact person.

15 November 2000

(4) Shift Commander will be briefed by first officer on the scene and make his/her evaluation of the situation. If it is determined to be a valid threat, the Shift Commander will have the dispatcher make emergency notifications using the Notification Matrix.

(5) Shift Commander will remain on scene with his/her police personnel and assume duties as on-scene-commander until the arrival of the Security Officer or NADO.

(6) Upon arrival of the on-scene-commander, security personnel will be utilized to set up an inner perimeter, assist in the search of the facility, provide traffic control as required, and other duties as assigned.

e. USNA Fire Department

(1) If there is an actual bomb detonation, the Fire Department will conduct medical and fire fighting responsibilities. The senior Fire Department person on the scene will assume duties as Fire Fighting and Medical Commander until arrival of the Fire Chief or other competent authority.

(2) If there is only a bomb threat, fire personnel will stage their equipment away from the scene and await orders from the on-scene-commander.

15 November 2000

APPENDIX F

WEAPONS OF MASS DESTRUCTION

1. Purpose. To establish policy and procedures for the response and handling of Weapons of Mass Destruction (WMD) incidents.
2. General. Recent changes in international availability of chemical, and to a lesser extent biological agents, increases the possibility of a WMD incident. The threat of WMD terrorism is different than the threat of Nuclear Biological and Chemical attack on a battlefield. As events in Tokyo (1995 sarin attack), New York City (1993 World Trade Center) and Oregon (1984 salmonella bacterium attack) indicate, the use of chemical and biological agents in a terrorist attack are not only possible, but have been planned and executed. To a terrorist looking to terrorize, U.S. installations make inviting targets. Many areas on the Naval Academy tend to congregate unprotected people. Examples of these are anyplace where many people gather to attend any events, such as sport competitions, theaters, and official ceremonies.
3. Mission. Protection of life, government assets, and restoration of normal operations as rapidly as possible.
4. Execution
 - a. The first indication of a biological incident is most likely to be a significant increase of incidents of a specific ailment. Hospital emergency rooms may be the first to notice that a major incident has occurred. Investigators will try to identify the causing agent and a common occurrence in the victim's recent history that may have led to the ailment. The incident may have occurred several days or more before detection of the incident and no immediate response will be possible.
 - b. In the event of a suspected biological or chemical attack, USNA security forces will attempt to isolate the scene of the incident, maintaining a standoff range sufficient to limit the affects of the agent. Every attempt will be made to identify the agent. Once the agent is identified attempts will be made to neutralize the agent.
5. Responsibilities
 - a. Fire/Police Dispatcher
 - (1) Alert and dispatch USNA Fire Department and DOD Police to scene of incident.
 - (2) Contact the Anne Arundel County Hazardous Material response Unit, the Fort Meade Hazardous Material Response Team at (301) 677-2117, the National Response Center at 1-800-424-8002, and the Chemical Biological Incident Response Force (CBIRF) from Joint Forces Command Indian Head at 301-744-2036/7.
 - (3) Notify all personnel concerned using the Security Department Emergency Notification Matrix.

15 November 2000

(4) Remind responding units to maintain standoff distance until the agent can be identified and a safe zone is established.

b. Fire Department/Hazardous Material (HAZMAT) Response Teams

(1) The Duty Assistant Fire Chief will set up the Command Post and act as on-scene-leader until properly relieved. All response units will stage upwind at a minimum of 300 feet until a determination is made of the contaminant. Once the contaminant is identified, a safe zone will be established. All responding Fire Department personnel will be in full protective fire fighting gear and will have a Self Contained Breathing Apparatus (SCBA) available. Anne Arundel County and Fort Meade HAZMAT units will be equipped with Level "A" Contamination Suits (Moonsuits).

(2) An on-scene-command center will be placed upwind from the incident and an inner and outer perimeter will be established, where the outer perimeter will be used for the command center and for decontamination procedures. The inner perimeter will mark the "Hot Zone." An entry and egress area will be identified where anyone requiring access to either the inner or outer perimeter must pass. Security personnel will be utilized to limit access and keep track of people as they leave and enter the scene. Marines in Personal Protective Clothing and masks will be utilized to control access where contamination is most likely.

(3) Decontaminations stations will be set up by the Anne Arundel County and Fort Meade HAZMAT units in the outer perimeter, and at a minimum of 300 feet upwind of the source until a safe zone is established. The USNA Fire Department will provide assistance utilizing the HAZMAT Support Trailer.

(4) Victims of the attack will be decontaminated by Anne Arundel County, Fort Meade and USNA HAZMAT Response units prior to being transported to a medical facility. No one will be transported until it is determined the agent will not be spread. Anti-toxins will be administered if available.

c. Deputy for Operations. Upon receiving notification that a WMD incident has occurred the Deputy for Operations or, after normal working hours, and on weekends and holidays, the NADO will:

(1) Immediately assess the situation.

(a) Notify the Immediate Chain of Command.

(b) Notify the Chief of Naval Operations Duty Captain by voice WITHIN 5 MINUTES USING REFERENCE (a) OPREP-3 FORMAT.

(c) Notify the Commandant, Naval District Washington, DC (Operations/Duty Officer).

(d) Submit an initial Special Incident Report (OPREP-3 PINNACLE) message (within 20 minutes). Reference (a) provides detailed guidance on voice and message OPREP Reporting. A copy of reference (a) is maintained in the NADO briefcase along with formatted message guides for use by the Deputy for Operations and/or the NADO.

(e) Activate the EOC.

15 November 2000

(f) Order the Security Officer to increase THREATCON as required.

(2) If necessary, the Deputy for Operations will order an evacuation of the Academy. Depending on wind direction and the specific threat, personnel will be ordered to evacuate to a local site for further transportation to final evacuation locations. The two primary local evacuation sites are the USNA Stadium parking lot or NAVSTA. Initial evacuation to local evacuation sites will be by personal auto and foot. Once at the staging areas, transportation will be set-up to the final evacuations sites that are determined by Deputy for Operations.

d. Security Officer/NADO

(1) Assist the Fire Department with the evacuation of the incident area.

(2) Act as on-scene-commander, set up a perimeter using DOD Police, the Marine Reaction Force, ASF, and military personnel.

(3) Increase THREATCON as ordered by Deputy for Operations.

(4) Notify the NMCL to immediately initiate the Disaster Control Plan.

(5) Stand up the EOC.

(6) Contact the Resident Agent of NCIS.

(7) Establish a landing zone for response units and emergency services.

e. DOD Police

(1) Respond to scene, maintain appropriate standoff.

(2) Set up a perimeter, provide traffic control as required and other duties as assigned.

f. Cost-center Heads

(1) Have a written evacuation plan posted in conspicuous areas of the buildings and ensure that all occupants of the building are aware of the plan.

(2) Have designated evacuation routes marked, indicating they are evacuation routes.

(3) Ensure that the evacuation does not put the occupants at greater risk.

(4) Have emergency evacuation signal, ensure all occupants are aware of the signal.

(5) Have designated areas outside and a safe distance from the building being evacuated where supervisors can account for their assigned personnel.

g. Public Works Officer. Have personnel on standby to:

(1) Provide a portable public address system to the on-scene-commander.

15 November 2000

(2) Provide equipment and personnel under the control of the Public Works Department as requested by the on-scene-commander including emergency lighting, heavy equipment, evacuation vehicles, etc.

h. Public Affairs Officer. The PAO will coordinate all aspects of relations with news media under the direction of the Deputy for Operations and the on-scene-commander.

APPENDIX G

Training

1. Purpose. To establish policy and procedures for Command Force Protection Training.

2. General. The Superintendent has a continuing responsibility to ensure that personnel receive comprehensive security awareness briefings. The objective is to develop the installation security awareness to such a degree that the organization presents a very strong security profile. In so doing, it becomes a significantly less vulnerable target.

a. Security awareness and personnel protection programs are to increase awareness of the possible threat of terrorism. The Force Protection Officer (FPO) is charged with keeping all DOD personnel, including dignitaries, civilian employees, and family members, aware of the general threat, as well as the perceived threat level in the general area of the installation.

b. All military personnel and family members, as well as civilians connected with the military or U.S. Government (including contract personnel), are potential victims of terrorist attack and should take the proper security precautions. The most important measure is educating persons who are likely targets in the recognition of a threat and taking appropriate actions to reduce their risk. Personal protection, education, and training must emphasize how to deny the opportunity for an attack or to elevate the risk to the attacker.

3. Mission. A comprehensive security education program must view security as part of operations, training, quality of life and health, morale and welfare activities. In addition, it must include physical security measures for crime prevention, pilferage, operational security, as well as personnel security and the collection, analysis and reporting of intelligence information relating to domestic and international terrorism incidents. Responsibility for the education program extends beyond the physical parameters of the installation, emphasizing close coordination and association with law enforcement officials and includes the military population in the community at large.

4. Execution

a. Level II Training. The Superintendent shall ensure that the installation FPO is a commissioned officer or civilian equivalent (GS-11 or above) and has attended the FPO course (J-830-0015). This training is mandatory and is recognized by DOD as Level II Force Protection/Antiterrorism (FP/AT) training. It is a dual certification course in FP and Antiterrorism Training. Upon completion, the FPO will demonstrate the ability to use approved and standardized procedures to provide antiterrorism and individual protective measures (Level I) training to all DOD military and civilian personnel. In addition, the FPO will be trained to formulate, organize, and maintain a comprehensive antiterrorism and FP plan tailored to the specific needs of the command.

b. Level I Training. The FPO is responsible for the Level I training aboard the installation. The FPO may be assisted in this endeavor by those persons who have attended the Antiterrorism Training Officer Course (J-830-0010) which provides

15 November 2000

the individual with the skills to use approved and standardized procedures to provide antiterrorism and individual protective measures training.

(1) Individual training will consist of a program that makes the personnel aware that a threat is present and that they must be constantly aware that they, the installation personnel, are the command's first line of defense against the gathering of intelligence on them. The following are DOD mandatory, standardized, Level I training topics:

- (a) Introduction to Terrorism.
- (b) Terrorist Operations.
- (c) Individual Personnel Protection Measures.
- (d) Terrorist Surveillance Techniques.
- (e) Hostage Survival.
- (f) Explanation of Threat Level.
- (g) Recent Area of Responsibility Updates for area of travel.

(2) The FPO shall ensure that a certified FPO/ATTO provides assigned personnel, military/DON civilian and adult family members with AT/FP training within 6 months prior to deploying, transferring overseas, or traveling outside the United States, its territories, and possessions. This includes deployment, temporary additional duty, permanent change of station, and leave. Adult family members are defined as someone at least 16-years old or an age or maturity level deemed appropriate by the sponsor or guardian. Issuance of the Joint Staff Guide 5260 is required and all personnel will view the video "Out of Harm's Way."

(3) If Threat Levels in the United States or its territories or possessions rise above the level of negligible, the FPO will ensure that Level I training is conducted annually by a certified FPO/ATTO for all personnel associated with the installation and the JS Guide 5260 will be made available to all personnel.

c. Security Force Training. The FPO, in coordination with the NAVSTA Security Officer, will ensure that the ASF maintains staffing at required levels. They will ensure that all ASF personnel are proficient in the handling of small arms and that they have received comprehensive "Use of Deadly Force" training. They will be thoroughly familiar with the installation layout and their responsibilities when activated in a FP role. The CO, Marine Barracks is charged with ensuring that all Marine Security Force Company personnel are trained and proficient, in accordance with Marine Corps Orders, to carry out their mission as a final barrier to selected locations when activated.

d. Exercises and Drills. In compliance with CNO directives, the Superintendent shall ensure that the entire Force Protection Plan (FPP) is exercised annually to ensure the installation's readiness and capability to detect, deter, and/or defend

against a terrorist attack. Exercises also serve to evaluate response efforts and consequence management during and after a terrorist attack. Additionally, portions of the FPP shall be exercised quarterly and during each increase in THREATCON during duty and nonduty hours. This will ensure that the physical security portion of the plan is consistent with local minimum standards. Exercises will involve NCIS, fire, medical, explosive ordnance, disaster preparedness, and local agencies to the greatest extent possible.

APPENDIX H

Emergency Operations Center

1. Purpose. To establish policy and procedures for manning the EOC.
2. General. The EOC is located in the Public Safety Building (Bldg # 257), Room 106. The EOC will be manned during significant incidents concerning the security and safety of the United States Naval Academy Complex and personnel and in the case of a natural disaster.
3. Execution
 - a. The Deputy for Operations will order the Security Officer to establish the EOC under the following conditions:
 - (1) THREATCONS CHARLIE and DELTA.
 - (2) Civil disturbance.
 - (3) Hostage situation.
 - (4) Sabotage.
 - (5) Bombs, bomb threats, and explosions.
 - (6) Weapons of mass destruction.
 - (7) Mass casualty.
 - (8) Natural disaster.
 - b. The following personnel or designated departmental representative will man the EOC under all circumstances. After assessing the situation the Base Operations Officer will decide who will not be required.
 - (1) Base Operations Officer or NADO.
 - (2) Security Officer or Chief of Police.
 - (3) Fire Chief or Assistant Fire Chief.
 - (4) Physical Security Specialist.
 - (5) CO, Marine Barracks.
 - (6) NMCL.
 - (7) CBU-403.

15 November 2000

(8) NAVSTA Executive Officer or Security Officer.

(9) PAO.

(10) Public Works.

(11) Family Service Center.

(12) Commandant Staff.

c. The following personnel or designated departmental representative will man the EOC when directed.

(1) Information Technology.

(2) NCIS.

(3) Staff Judge Advocate.

(4) NAAA.

(5) Housing Officer.

(6) Supply Officer.

H-2

Enclosure **(1)**
Appendix (H)

For Official Use Only

DEPARTMENT OF THE NAVY

TELEPHONIC THREAT COMPLAINT

IF BOMB THREAT, ASK THE CALLER

- WHEN IS THE BOMB TO GO OFF?
- WHERE IS THE BOMB TO GO OFF?
- WHAT KIND OF BOMB IS IT?
- WHAT DOES THE BOMB LOOK LIKE?
- WHERE ARE YOU CALLING FROM?

1. COMMAND			
a. Name & Address		b. Phone No.	
2. COMPLAINANT			
a. Name			
3. PERSON RECEIVING CALL			
a. Name		b. Date & Place of Birth	
c. Command Name & Address		d. Phone Number (Work)	(Home)
4. TELEPHONE CALL RECEIVED ON			
a. Phone Number (Include area code)		b. Location	
c. Phone number listed in ("X" all that apply)			
<input type="checkbox"/> Unlisted <input type="checkbox"/> Other (List) <input type="checkbox"/> Command Directory <input type="checkbox"/> Base Directory <input type="checkbox"/> Local Directory			
5. DETAILS OF CALL			
a. Date		b. Day of Week	c. Time
6. CONTEXT OF CONVERSATION			
a. Recipient "			"
b. Caller "			"
c. Recipient "			"
d. Caller "			"
e. Recipient "			"
f. Caller "			"
7. BACKGROUND NOISES (Describe street sounds, voices, music, etc. If more space needed, continue on reverse.)			
8. INFORMATION ABOUT CALLER/VOICE CHARACTERISTICS			
a. Sex	b. Age	c. Race	d. Accent
e. Educational Level		f. Attitude (Calm, Nervous, Serious)	
g. Other			
9. WERE THERE ANY WITNESSES TO THE CALL?		10. DO YOU HAVE ANY SUSPICION AS TO THE IDENTITY OF THE CALLER?	
<input type="checkbox"/> No <input type="checkbox"/> Yes (List Name)		<input type="checkbox"/> No <input type="checkbox"/> Yes (List Name)	
11. NOTIFICATION OF AUTHORITY ("X" all notified)			
<input type="checkbox"/> CO	<input type="checkbox"/> XO	<input type="checkbox"/> OOD	<input type="checkbox"/> Security
<input type="checkbox"/> NISRA	<input type="checkbox"/> Telephone Co.	<input type="checkbox"/> EOD	<input type="checkbox"/> Fire Dept.

CLEAR