



DEPARTMENT OF THE NAVY

NAVAL AIR STATION
POINT MUGU, CALIFORNIA 93042-5000

FOR OFFICIAL USE ONLY

NASPTMUGUINST 5530.7

6500

8 March 1990

FOR OFFICIAL USE ONLY

NAS POINT MUGU INSTRUCTION 5530.7

From: Commander Officer

Subj: ANTITERRORISM, HOSTAGE CRISIS, OR BARRICADED CRIMINAL SITUATIONS

Ref: (a) OPNAVINST 5530.14B
(b) SOP/LACINST 3440.2E
(c) SOP/LACINST 3100.1M

Encl: (1) Terrorist Threat Conditions for Combatting Terrorism

1. Purpose. To establish procedures to be implemented for the prevention, containment, and resolution of acts of terrorism, hostage crisis, or barricaded criminal element situations on the Point Mugu Complex.

2. Cancellation. COMPMTINST 5530.1

3. Discussion. Reference (a) directs Commanding Officers to develop and promulgate procedures and assign responsibilities to prevent, respond to, and counter acts of terrorism. Certain similarities exist among the tactics and goals of terrorists to those used in hostage or barricaded criminal situations which require guidelines directed at resolving these crises. Each of these situations requires specific planning for prevention, containment, and resolution as outlined in enclosure (1). Reference (b) issued procedures for general alert.

4. Responsibilities

a. Security Officer (Code 6500) is assigned the responsibility for implementing and enforcing the procedures outlined in this instruction. During terrorist, hostage crisis, or barricaded criminal situations, he shall proceed to the Crisis Management Command Center and take the required actions to:

- (1) Monitor all security response personnel, Civilian/Military Police and Auxiliary Security Force.
- (2) Support the Hostage Negotiation Team.
- (3) Furnish weapons and ammunition as required.
- (4) Furnish a debriefing team and advise the Commanding Officer of pertinent information obtained.
- (5) Coordinate with Pacific Missile Test Center (PMTIC) Surface Craft Division for rescue boats when necessary.
- (6) Coordinate with allied law enforcement agencies.

b. Heads of Commands, Directorates, and Tenant Organizations and Activities shall render maximum practicable assistance as required and coordinate with the Naval Air Station (NAS) Security Officer for the purpose of developing preventive measures and training of assigned personnel in Preventative Reactionary Measures to terrorist, hostage, or barricaded criminal situations.

c. Officer of the Day (OOD) shall:

- (1) Assume command control until relieved by the Commanding Officer or Executive Officer, NAS.
- (2) Assure that notification directed in paragraph 6 below is completed.
- (3) Maintain a log of events, orders issued, actions taken, etc.
- (4) Activate the Crisis Management Command Center (conference room, Building 1). During working hours, use the Personnel Support Activity Detachment (PSD) personnel; after hours, the Assistant OOD (AOOD).
- (5) Assist the PMTC CDO with reports required by reference (c).

FOR OFFICIAL USE ONLY

d. Security Police Supervisor shall:

- (1) Assume on-scene tactical command of the crisis situation until relieved by Police Chief, Head of Law Enforcement Operations Division, or person designated by the Commanding Officer.
- (2) Assume control of outer perimeter and assist the on-scene tactical commander when relieved as on-scene tactical commander.
- (3) Direct all radio communications to be restricted to emergency traffic only.

e. Police Chief, Head of Law Enforcement Operations Division, or person designated by the Commanding Officer shall:

- (1) Assume on-scene tactical command of the crisis situation until relieved by the FBI.
- (2) Provide updated information to the crisis management command center.
- (3) Contain the situation until resolved.

f. Medical Officer shall ensure Emergency Medical Technicians are in an alert status.

g. Officer In Charge, Explosive Ordnance Disposal (EOD) shall ensure EOD personnel are readily available to respond as directed by the Commanding Officer.

h. Public Works Officer (Code 6200) shall:

- (1) Proceed to the Crisis Management Command Center.
- (2) Take the required action to control all utilities (telephone, water, electricity, sewer, etc.) in the situation area or building as required.
- (3) Furnish transportation and vehicles as required.

i. Supply Officer (Code 6300) shall:

- (1) Proceed to the Crisis Management Command Center.
- (2) Take the required action to provide Supply Department support to include messing.

j. Administration Officer (Code 6800) shall:

- (1) Proceed to the Crisis Management Command Center.
- (2) Take the required action to provide personnel support (manpower) and berthing.

k. PSD personnel shall:

- (1) Proceed to and activate the Crisis Management Command Center.
- (2) Furnish personnel to support the Crisis Management Command Center as required by the PMTC Disaster Preparedness Plan.
- (3) Furnish information as required from service records of military personnel.

l. Air Operations Officer (Code 6100) shall:

- (1) Proceed to the Crisis Management Command Center and take the required actions for the support of:
 - (a) Aircraft.
 - (b) Fire and Crash Crews.
 - (c) Ground Electronics (emergency installation and repairs to radio equipment).

m. Legal Officer (Code 6008) shall proceed to the Crisis Management Command Center and provide legal advice to the Commanding Officer.

n. Public Affairs Coordinator shall proceed to the Crisis Management Command Center; provide advice to the Commanding Officer; and coordinate Public Affairs with the PMTC Public Affairs Officer.

o. Officer In Charge, San Nicolas Island shall publish a Contingency Plan for the immediate response to a terrorist, hostage, or barricaded criminal situation until arrival of trained support personnel as designated in this instruction.

p. Naval Investigation Services (NIS) shall:

- (1) Proceed, if available, to the Crisis Management Command Center.
- (2) Provide advisory services to the Commanding Officer.
- (3) Provide intelligence gathering about terrorist groups, hostage taker, hostage, scene, etc.
- (4) Provide trained hostage negotiators.
- (5) Provide liaison with other law enforcement agencies.
- (6) Provide arrest team.
- (7) Provide follow-up investigation.

5. Terrorist Threat Condition (THREATCON)

a. Threat Condition Alpha: This condition applies when there is a general threat of possible terrorist activity against installations and personnel, the nature and extent of which are unpredictable, when circumstances do not justify implementation of the measures of threat condition Bravo. However, it may be necessary to implement certain selected measures from threat condition Bravo as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

b. Threat Condition Bravo: This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in 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.

c. Threat Condition Charlie: This condition applies when an incident occurs or when intelligence is received indicating that some form of terrorist action against installations and personnel is imminent. Implementation of this measure for more than a short period will probably create hardship and will affect the peacetime activities of the unit and its personnel.

d. Threat Condition Delta: This condition 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 threat condition is declared as a localized warning.

6. Action

a. The Commanding Officer will set THREATCON levels predicated upon intelligence reports, threat receipt, or direction of higher authority, as appropriate. Notification of changes in THREATCON levels shall be accomplished by the OOD or AOOD through the duty officer of tenant activities and NAS department heads.

b. Any person having knowledge of any information related to actual, attempted, or impending threat of a terrorist, hostage, or barricaded criminal nature shall immediately report all information to the OOD or AOOD, telephone 989-7209/7294. The OOD or AOOD shall notify personnel in the following order:

- (1) Security Police Dispatcher, who will notify:
 - (a) Security Officer, who will notify the FBI as required.
 - (b) Auxiliary Security Force.
 - (c) NIS Port Hueneme.
 - (d) Command Negotiators.

FOR OFFICIAL USE ONLY

NASPTMUGUINST 5530.7

8 March 1990

(2) Commanding Officer and Executive Officer.

(3) PMTC CDO.

(4) Department Heads:

(a) Air Operations Department.

(b) Public Works Department.

(c) Supply Department.

(d) San Nicolas Island Department.

(e) Administration Department.

(5) Branch Clinic (place on alert).

(6) Officer In Charge, PSD.

(7) Legal Officer.

(8) Public Affairs Coordinator.

(9) EOD Group One (place on alert).

7. Operations Procedures

a. Command Control Center. The Crisis Management Command Center is located in the Conference Room, Building 1. The Crisis Management Command Center will provide the Commanding Officer with adequate communications to direct operations and coordinate supportive actions for the control and resolution to counter terrorism, barricaded captor, or hostage crisis situations.

(1) The Crisis Management Command Center radio and telephone communications, when activated, consist of:

(a) Telephone (Class A) - extensions 7903/7904/7505/8607 and 8031.

(b) Magnetic telephone, a direct phone between the Crisis Management Command Center and Air Operations Officer, Fire Chief, Crash Crew, Public Works Officer, Shops Superintendent, Transportation Officer, Supply Officer, Security Officer, Branch Clinic, EOD, and the Disaster Preparedness warehouse.

(c) Radio

(1) Security Net, call sign "Veedal tango 37,"

(2) Mugu Net, (Crash/Fire/Rescue) call sign "Mugu 99."

(2) The Temporary Crisis Management Command Center will be the OOD Office, Building 1, until the Crisis Management Command Center is activated. If Building 1 is the incident area, Building 55 will be the Alternate Crisis Management Command Center.

b. On-Scene Command Post. The choice of a Command Post will depend on the location of the incident and adequacy of communications and protection. The on-scene Commander will locate the on-scene Command Post in an appropriate area in the vicinity of the crisis incident, based on cover, communications, accessibility and other tactical considerations.

c. Communication

(1) The command primary communication will be Security Net 1 or 2, in Digital Encryption Standard.

(2) Telephone systems will be used by the Hostage Negotiation Team. Radio communications may be required during an aircraft hijacking situation.

(3) In the event the Security Net is compromised, the Mugu Net will be used for communication.

FOR OFFICIAL USE ONLY

8. Training and Readiness

a. Security Officer shall:

- (1) Plan, schedule, and conduct drills as required.
- (2) Ensure all response personnel maintain a proper level of readiness.

b. Response personnel listed in paragraphs 4 and 5 of this instruction shall ensure that personnel under their cognizance are indoctrinated, trained, and capable of performing their assigned duties.

9. Reports Reports shall be completed in accordance with reference (c). The requirements contained in reference (c) are exempt from reports control and requires no report symbol.

Distribution:
A-3



D. L. SOLOMON

TERRORIST THREAT CONDITIONS FOR COMBATTING TERRORISM
CNO MSG 0317082 APR 86

Threat Condition Alpha: This condition applies when there is a general threat of possible terrorist activity against installations and personnel, the nature and extent of which are unpredictable, when circumstances do not justify implementation of the measures of threat condition Bravo. However, it may be necessary to implement certain selected measures from threat condition Bravo as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

Threat Condition Bravo: This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in 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.

Threat Condition Charlie: This condition applies when an incident occurs or when intelligence is received indicating that some form of terrorist action against installations and personnel is imminent. Implementation of this measure for more than a short period will probably create hardship and will affect the peacetime activities of the unit and its personnel.

Threat Condition Delta: This condition 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 threat condition is declared as a localized warning.

Guidelines provided for uniform implementation of Security Alert conditions. Assessment Factors:

A. Existence: a terrorist group is present in the area of concern, group need not have posed a threat to U.S. or DOD interest in the past.

B. Capability: a terrorist group has the ability to carry out an operation against U.S. interests in areas of concern. This includes resources such as intelligence, mobility, personnel, etc.

C. History: A group's history of terrorist acts and behavior reflects an anti-U.S. stand or include previous attacks against U.S. interests.

D. Trends: A group has, over the past year, displayed significant terrorist activity that appears to be continuing or increasing. Activity need not be violent; e.g., threat statements or utterances. This factor could be flexible depending on the length of the group's activity cycle.

E. Targeting: There are known plans or confirmed intentions of a terrorist group to target U.S. or DOD interest, specific or non-specific. If targeting is not against U.S. or DOD interest, this factor should not be considered.

Measures for Threat Conditions

1. At regular intervals, remind all personnel including dependents, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; alert for unidentified vehicles on or in the vicinity of, U.S. installations, and alert for abandoned parcels or suitcases or any unusual activity. (A-B-C-D)

2. Keep available at all times the Duty Security Officer, or other appointed personnel, who have access to plans for evacuating buildings and areas in use for sealing off any areas where an explosion or attack has occurred. Keep all key personnel who may be needed to implement security plans on call. (A-B-C-D)

3. Secure buildings, rooms, and storage areas not in regular use. (A-B-C-D)

4. Increase security spot checks of vehicles and persons entering the installation and nonclassified areas under the jurisdiction of the U.S. command and agency. (A-B-C-D)

5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic. (A-B-C-D)

Enclosure (1)

FOR OFFICIAL USE ONLY

8 March 1990

6. As a deterrent, apply one of the following measures from threatcon bravo individually and randomly.
 - A. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.
 - B. At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages.
 - C. Check all deliveries to messes, clubs, etc. (advise dependents to check all home deliveries)
 - D. As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs and other soft targets to improve deterrence and defense and to build confidence among staff and dependents. (A-B-C-D)
7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of the higher threatcon. (A-B-C-D)
8. Review and implement, as appropriate security measures for high risk personnel. (A-B-C-D)
9. Spare.
10. Repeat measure 1 and warn personnel of any other form of attack to be used by terrorist. (B-C-D)
11. Keep all personnel involved in implementing anti-terrorist contingency plans on call. (B-C-D)
12. Check plans for implementation of the measures contained in next threatcon. (B-C-D)
13. Centralize parking. (B-C-D)
14. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use. (B-C-D)
15. At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages. (B-C-D)
16. Examine all mail for letter or parcel bombs. (above normal) (B-C-D)
17. Check all deliveries to messes, clubs, etc. and advice all dependents to check all home deliveries. (B-C-D)
18. As far as resources allow, increase surveillance of domestic accommodations, schools, messes clubs and other soft targets to build confidence among staff and dependents. (B-C-D)
19. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm. (B-C-D)
20. At an early stage, inform members of local security committees of any action being taken and why. (B-C-D)
21. Upon entry of visitors to the unit, physically inspect them and a percentage of their suitcases, parcels, and other containers. (B-C-D)
22. Wherever possible, operate random patrols to check vehicles, people and buildings. (B-C-D)
23. Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive a car. (B-C-D)
24. Implement additional security measures for high risk personnel, as appropriate. (B-C-D)
25. Brief personnel who may augment guard force on use of deadly force. (B-C-D)
26. SPARE.

Enclosure (1)

FOR OFFICIAL USE ONLY

NASPTMUGUINST 5530.7
8 March 1990

27. SPARE.
28. SPARE.
29. SPARE
30. Continue all bravo threatcon measures or introduce those outstanding. (C-D)
31. Keep available at their place of duty all personnel who are responsible for implementing antiterrorist plans. (C-D)
32. Limit access points to absolute minimum. (C-D)
33. Strictly enforce control of entry and search a percent of vehicles. (C-D)
34. Enforce centralize parking of vehicles away from sensitive buildings. (C-D)
35. Issue weapons to guards. (Local orders for issue of ammo.) (C-D)
36. Introduce increased patrolling of the installation. (C-D)
37. Protect all designated vulnerable points and give special attention to vulnerable points outside military establishment. (C-D)
38. Erect barriers and obstacles to control traffic flow. (C-D)
39. SPARE.
40. Continue or introduce all measures for threatcon bravo and charlie. (D)
41. Augment guards as necessary. (D)
42. Identify all vehicles already on the installation within operational or mission support areas. (D)
43. Search all vehicles entering the complex or installation as well as the vehicles contents. (D)
44. Control all access and implement positive identification of all personnel. (D)
45. Search all suitcases, briefcases, packages, etc., brought into the complex or installation. (D)
46. Take measures to control access to all areas under the jurisdiction of the U.S. Command or agency. (D)
47. Make frequent checks of the exterior of concerned buildings and of parking lots. (D)
48. Minimize all administrative journeys and visits. (D)
49. Consult local authorities about closing public and military roads and facilities that might make sites vulnerable to terrorist attack. (D)
50. SPARE.

Enclosure (1)

FOR OFFICIAL USE ONLY