TABLE OF CONTENTS

Mandatory Antiterrorism/Force Protection Standards	1
Elements of the Combating Terrorism Program	5
Antiterrorism Threat Level Factors/Threat Levels	6
Antiterrorism Threat Conditions (THREATCONs)	7
Shore-Based Terrorist Threat Conditions	8
Shipboard Terrorist Threat Conditions	13
Pre-Port Arrival Procedures for Afloat Units	21
Pre-Arrival Procedures for Aircrews	22
Pre-Port Arrival Procedures for Small Command OiC's	23
Training	24
Navy IG Special Interest Item: Antiterrorism Readiness	25
References	28
Emergency Phone Number Listings	29
Responsible Organizations	30

ANTITERRORISM/ FORCE PROTECTION

for Naval Operations

COMMANDER'S GUIDE

Force Protection is a program designed to protect ALL personnel, facilities, and equipment under all situations and at any location. To accomplish this goal commanders must plan, integrate, and apply all in-place programs (i.e., combatting terrorism, physical security, security operations, personnel protective services, etc.) and support this effort through extensive use of available intelligence and counter-intelligence services.

The following mandatory standards are designed to assist commanding officers and commanders by increasing their awareness of requirements to enhance antiterrorism/force protection (AT/FP). The standards summarize steps necessary for quick and ready response to terrorist acts. A concise listing of mandated Standards is found in DoD 2000.XX

DoD Combating Terrorism Program Standards

1. **Combatant Commanders, Chiefs of Services and Directors of DoD Agencies (DoD Components) are responsible for the implementation of DoD Antiterrorism/Force Protection (AT/FP) policies within their organizations.** Full implementation of the spirit and intent of DoD policies will, in most cases, require DoD Components to develop additional antiterrorism force protection standards.

2. **DoD Components will clearly establish operational responsibility for AT/FP for all units and individuals whether permanently or temporarily assigned.**

3. **DoD components will fully coordinate their AT/FP efforts with host nation authorities and the U.S. Country Team.**

4. **DoD Components will develop and implement a comprehensive AT/FP program designed to accomplish all the standards contained in this document.** The program will include a series of well-defined plans that describe and implement the program.

5. **DoD Components will schedule a higher headquarters level assessment of their installations and AT/FP Programs at least once every three years.**

Service or combatant commanders must comply with this standard.

Commanding Officers (installation, unit, ship) must comply with this standard, as aplicable.

6. **Commanders at all levels will use the DoD Terrorist Threat Level Classification system to identify the terrorist threat in a specific overseas country.**

7. **Commanders will task the appropriate organizations under their command to collect, analyze and disseminate terrorist threat information as appropriate.**

8. **Commanders will prepare a terrorist threat assessment plan for their area of responsibility.**

9. **Commanders will ensure all information pertaining to terrorist threats, or acts of terrorism involving DoD personnel or assets in their AOR, is forwarded through the chain of command or line of authority as appropriate.**

10. **Commanders will develop a process, based on terrorist threat information and/or guidance from higher headquarters, to raise or lower THREATCON levels.**

11. **DoD Components will ensure that THREATCON transition procedures and measures are properly disseminated and implemented by subordinate commanders within their AOR.**

12. **Commanders will develop measures or actions for each THREATCON level as the threat situation increases from THREATCON NORMAL to THREATCON DELTA.**

13. **Commanders will prepare a terrorist physical security vulnerability assessment for facilities, installations and operating areas within their area of responsibility.** The assessment will address the broad range of physical threats to the security of personnel and assets.

14. **Commanders will develop and implement a physical security plan, as part of the AT/FP program, that incorporates facilities, equipment, trained personnel and procedures into a comprehensive effort designed to provide maximum antiterrorism protection to personnel and assets.**

15. **Commanders will exercise the physical security and force protection plan and terrorist incident response plan to determine their ability to protect personnel and assets against terrorist attack.**

16. **All commanders will routinely review the effectiveness of daily physical security measures under THREATCON NORMAL.**

17. Commanders will ensure DoD personnel assigned to Medium or High Terrorist Threat Level areas, and not provided on-installation or other government quarters, are furnished guidance on the selection of private residences to mitigate risk of terrorist attack.

18. Commanders in Medium or High Terrorist Threat Level areas will conduct physical security assessments of off-installation residences for permanently and temporary duty DoD personnel. Based on the assessment results, commanders will provide AT/FP recommendations to residents and facility owners.

19. DoD Components will establish AT/FP guidelines for new construction to counter terrorist threat capabilities within the AOR.

20. Commanders will develop a prioritized list of AT/FP factors for site selection teams. These criteria will be used to determine if facilities, either currently occupied or under consideration for occupancy by DoD personnel, can adequately protect occupants against terrorist attack.

21. A pre-deployment AT/FP vulnerability assessment will be conducted for all units prior to deployment. Commanders will implement appropriate force protection measures to reduce risk and vulnerability.

22. Commanders will ensure that all personnel under their command receive the appropriate training for individual antiterrorism awareness prior to deploying or traveling outside the United States, its territories and possessions. The individual's records will be updated in accordance with DoD Component policy. Family members will receive similar training prior to traveling outside the United States, its territories and possessions on official government orders.

23. DoD Components will ensure that a Force Protection Officer, responsible to the Commander for AT/FP requirements, is assigned at each installation or base, and deploying organization (e.g., battalion, ship, squadron).

24. Combatant Commanders with geographic responsibilities will ensure DoD personnel entering their AOR have been provided country-specific guidance on antiterrorism protection.

25. Combatant Commanders with geographic responsibilities will ensure personnel designated as *personnel at high risk to terrorist attack and personnel assigned to high risk billets* receive appropriate AT/FP training prior to assuming duties.

26. Commanders will ensure DoD personnel and dependents assigned to Medium and High Threat locations are given guidance, at least annually, on appropriate conduct in the event they are taken hostage or kidnapped.

27. Commanders will prepare installation-wide terrorist incident response plans. These plans will include procedures for determining the nature and scope of post-incidence response measures, and plans to reconstitute the installation's ability to perform AT/FP measures.

28. Commanders will ensure Terrorist Incident Response plans contain current residential location information for all DoD personnel and their dependents assigned to Medium and High Terrorist Threat Level areas. Such plans will provide for enhanced security measures and/or possible evacuation of DoD personnel and their dependents.

29. Commanders will be familiar with treaty, statutory, policy, regulatory and local constraints on the application of supplemental security measures for executives. Commanders will take necessary measures to provide appropriate protective services for executives in high risk billets and high risk personnel in their AOR. *Review and revalidation of protective services will occur on at least an annual basis.*

30. DoD Components will develop estimates for potential terrorist use of Weapons of Mass Destruction (WMD) in their AOR. Reports through the chain of command and line of authority will be processed immediately when significant information is obtained identifying organizations with WMD capabilities operating in their AOR.

31. Commanders will assess the vulnerability of installations, facilities and personnel within their AOR to terorist use of WMD. Such assessments will address potential use of chemical, biological or radiological agents.

32. Commanders will take appropriate measures to protect DoD personnel and reduce the vulnerability to terrorist use of WMD. Commanders will exercise applicable measures as part of an antiterrorism and force protection program.

33. DoD Components shall use these standards as a baseline to develop specific standards with their unique requirements to fully implement their AT/FP program. As a minimum they should address plans, procedures to identify physical security requirements, program for resources to meet security requirements and new construction.

Elements of the Combating Terrorism Program (from DoDD 2000.12):

Ensure the training of commanders on an integrated systems approach to physical security and force protection technology.

Ensure that training on an integrated systems approach for force protection technology is included in planning for the acquisition of new facilities, AT systems, and individuals and equipment.

Ensure that all Service installations and activities utilize DoD 2000.12-H to develop, maintain and implement force protection efforts that familiarize personnel with DoD procedures, guidance and instructions.

Ensure that existing physical security, base defense and law enforcement programs address terrorism as a potential threat to Service personnel and their families, facilities and other DoD material resources.

Ensure each installation or base and/or ship has the capability to respond to a terrorist incident.

Ensure installations and/or ships conduct operational command post exercises annually.

Ensure every commander regardless of echelon, plans, resources, trains, exercises and executes antiterrorism measures outlined in referenced DoD and Joint Publications.

Ensure the training of individuals and specified personnel.

Antiterrorism Threat Level Factors

Threat levels are obtained based on the presence of a combination of Threat Analysis factors. DoD has developed a methodology to assess the terrorist threat to DoD personnel, facilities, material and interests. The factors are listed as follows:

THREAT LEVELS

- *The degree of risk to personnel, faacilities, assets or interest*
- Threat analysis performed by intel at each level of command.
- Threat Levels can differ at each ECHELON.
- Senior intelligence officer declares THREAT LEVELS.

Threat Level	Threat Analysis Factors				
	Existence	Capability	History	Intentions	Targeting
Critical	X	X	O	O	X
High	X	X	X	X	
Medium	X	X	X	O	
Low	X	X	O		
Negligible	O				

X Factor MUST be present O Factor MAY or MAY NOT be present

- EXISTENCE: Terrorist group is present or can gain access.
- CAPABILITY: Demonstrated capability to conduct terrorist acts.
- HISTORY: Demonstrated terrorist activity over time.
- INTENTIONS: Demonstrated anti-US terrorist activity.
- TARGETING: Credible information on specific terrorist operations.

Terrorist threat levels do not address when a terrorist attack will occur and do not specify a THREATCON status. (Issuance of a terrorist threat-level judgment is not a warning notice. Formal terrorism warning notices are issued separately.) Terrorist Threat Levels are listed:

- CRITICAL - Factors of Existence, Capability and Targeting must be present. CRITICAL is differentiated from all other terrorist threat levels because it is the only one in which credible information identifying specific DoD personnel, facilities, assets, or interests as potential targets of attack is present. Although particular action is not specified, a CRITICAL threat level compels local commanders to take appropriate protective measures.
- HIGH – Factors of Existence, Capability, History and Intentions must be present, but analysts lack specific targeting information.
- MEDIUM - Factors of Existence, Capability and History must be present. Threat level MEDIUM and threat level HIGH are similar in that data for the factors Existence, History and Capability exist.
- LOW - Existence and Capability must be present. History may or may not be present.
- NEGLIGIBLE - Existence and Capability may or may not be present.

Antiterrorism Threat Conditions (THREATCONs)

Whereas the Terrorist Threat Level is an intelligence community judgment about the likelihood of terrorist attacks on DoD personnel and facilities, the **THREATCON** *is the principal means a commander has to apply an operational decision on how to guard against the threat.* Ultimately it is the commander who must weigh the information and balance increased security measures with the loss of effectiveness during prolonged operations and the accompanying impact on quality of life.

THREATCONS are selected assessing the terrorist threat, the capability to penetrate existing physical security systems at an installation, the risk of terrorist attack to which DoD facilities personnel expose themselves, the ability of the installation or unit to carry with missions even if attacked, and criticality to DoD missions of assets being protected.

THREATCONs can be established by commanders at any level, a subordinate commander can establish a higher THREATCON if local conditions warrant doing so. THREATCON measures are mandatory when declared and can be supplemented by additional measures. The declaration, reduction and cancellation of THREATCONs remain the exclusive responsibility of the commanders issuing the order. Once a THREATCON is declared, the following security measures are mandatory and implemented immediately. Commanders are authorized and encouraged to supplement these measures.

HOW COMMANDERS DETERMINE THREATCONS:

THREATCON Levels	Intel Summaries	Warning Reports	Spot Reports	Law Enforcement Information
Normal Alpha Bravo Charlie Delta	Threat Information Coupled with Best Judgement ⇨ THREATCON LEVEL			

* **THREATCON NORMAL** exists when there is no know threat.

* **THREATCON ALPHA** exists when there is a general threat of possible terrorist activity against installations and personnel. The exact nature and extent are unpredictable and circumstances do not justify full implementation of THREATCON BRAVO. However, it may be necessary to implement selected THREATCON BRAVO measures as a result of intelligence or as a deterrent. THREATCON ALPHA must be capable of being maintained indefinitely.

* **THREATCON BRAVO** exists when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing hardship, affecting operational capability or aggravating relations with local authorities.

* **THREATCON CHARLIE** exists when an incident occurs or when intelligence is received indicating that some form of terrorist action is imminent. Implementation of this measure for longer than a short period of time will probably create hardship and affect peacetime activities of a unit and its personnel.

* **THREATCON DELTA** exists when a terrorist attack has occurred, or when intelligence indicates that a terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

SHORE-BASED TERRORIST THREAT CONDITIONS

1. The measures outlined below describe the progressive response to a terrorist threat to Department of the Navy facilities and personnel. These are common security measures designed to facilitate inter-Service coordination and support U.S. military antiterrorism activities.

2. The purpose of the THREATCON system is accessibility to, and easy dissemination of appropriate information. The declaration, reduction and cancellation of THREATCONs remains the exclusive responsibility of the commanders specified.

3. While there is no direct correlation between threat information, (e.g., Intelligence Summaries, Warning Reports and Spot Reports), and THREATCONs, such information, coupled with the guidance provided below, assists commanders and commanding officers in making prudent THREATCON declarations. Once a THREATCON is declared, the selected security measures are implemented immediately. The recommended measures are:

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

b. **THREATCON ALPHA** applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. It may be necessary to implement certain measures from higher THREATCONs resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

1. At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of United States installations. Watch for abandoned parcels or suitcases and any unusual activity.

2. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.

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

4. Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

5. Limit access points for vehicles and personnel commensurate with reasonable flow of traffic.

6. As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO either individually or in combination with each other.

7. Review all plans, orders, personnel details and logistics requirements related to the introduction of higher THREATCONs.

8. Review and implement security measures for high-risk personnel as appropriate.

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

10. To be determined.

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

11. Repeat Measure 1 and warn personnel of any other potential form of terrorist attack.

12. Keep all personnel involved in implementing antiterrorist contingency plans on call.

13. Check plans for implementation of next THREATCON.

14. Move cars and objects (e.g., crates, trash containers), at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.

15. Secure and regularly inspect all buildings, rooms and storage areas not in regular use.

16. At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

17. Examine mail (above the regular examination process) for letter or parcel bombs.

18. Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.

19. 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.

20. Make staff and dependents aware of the general situation to stop rumors and prevent unnecessary alarm.

21. At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

22. Physically inspect visitors and randomly inspect their suitcases, parcels and other containers. Ensure proper dignity is maintained, and if possible, ensure female visitors are inspected only be a female qualified to conduct physical inspections.

23. Operate random patrols to check vehicles, people, buildings and aircraft parking areas.

24. Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or exiting the vehicle.

25. Implement additional security measures for high-risk personnel as appropriate.

26. Brief personnel who may augment guard forces on the use of deadly force. Ensure there is no misunderstanding of these instructions.

27. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

28-29. To be determined.

d. **THREATCON CHARLIE** applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

30. Continue, or introduce, all measures listed in THREATCON BRAVO.

31. Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

32. Limit access points to absolute minimum.

33. Strictly enforce control of entry. Randomly search vehicles.

34. Enforce centralized parking of vehicles away from sensitive buildings.

35. Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

36. Increase patrolling of the installation.

37. Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.

38. Erect barriers and obstacles to control traffic flow.

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

40. To be determined.

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

41. Continue, or introduce, all measures listed for THREATCONs BRAVO and CHARLIE.

42. Augment guards as necessary.

43. Identify all vehicles within operational or mission support areas.

44. Search all vehicles and their contents before allowing entrance to the installation.

45. Control access and implement positive identification of all personnel- - NO EXCEPTIONS.

46. Search all suitcases, briefcases, packages, etc., brought into the installation.

47. Control access to all areas under jurisdiction of the United States.

48. Make frequent checks to exterior of buildings and parking areas.

49. Minimize all administrative journeys and visits.

50. Coordinate possible closing of public and military roads and facilities with local authorities.

51. To be determined.

SHIPBOARD TERRORIST THREAT CONDITIONS

1. The measures outlined below are for use aboard U.S. Navy vessels. These measures serve two purposes: first, the crew is alerted, additional watches are created, and there is greater security; second, these measures display the ship's resolve to prepare for and counter terrorist threats. The measures outlined below do not account for local conditions and regulations, special evolutions, or current threat intelligence. The command must maintain flexibility. As THREATCONs change, the ship must be prepared to take action to counter the threat. When necessary, additional measures must be taken immediately. While the simple solution to THREATCON CHARLIE or DELTA is to get underway, this option may not always be available.

2. The decision to arrive at a particular THREATCON is based on multiple factors that may include threat, target vulnerability, criticality of assets, security resource availability, operational and morale impact, damage control, recovery procedures, international relations and planned U.S. government actions that could trigger a terrorist response.

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

b. **THREATCON ALPHA** is declared when a general threat of possible terrorist activity is directed toward installations and personnel, the nature and extent of which are unpredictable, and where circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain selected measures from higher THREATCONs as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

1. Brief the crew on the threat, ship security and security precautions to be taken while ashore.

2. Muster and brief security personnel on the threat and rules of engagement.

3. Review security plans and keep them available. Keep key personnel who may be needed to implement security measures on call.

4. Consistent with local rules, regulations and status of forces agreement, post qualified armed fantail sentry and forecastle sentry. Rifles are the preferred weapon.

5. Consistent with local rules, regulations and status of forces agreement, post qualified armed pier sentry and pier entrance sentry.

6. Ensure two-way communications are established to all sentries, roving patrols, quarterdeck watch and response force. If practical, all guards shall be equipped with at least two systems of communication (e.g., two-way radio, telephone, whistle or signal light).

7. Issue night vision devices to selected security personnel.

8. Coordinate pier/fleet landing security with SOPA, co-located forces and local authorities. Identify anticipated needs for mutual support (security personnel, boats and equipment) and define methods of activation and communication.

9. Tighten shipboard and pier access control procedures. Positively identify all personnel entering pier/fleet landing area.

10. Consistent with local rules, regulations and status of forces agreement, establish unloading zone(s) on the pier away from the ship.

11. Deploy barriers to keep vehicles away from ship. Barriers may be ship's vehicles, equipment or items available locally.

12. Post signs in local languages to explain visiting and loitering restrictions.

13. Inspect all vehicles entering pier for unauthorized personnel, weapons and/or explosives.

14. Inspect all personnel, hand carried items and packages before they come aboard. Where possible, screening should be at pier entrance or foot of brow.

15. Direct departing and arriving liberty boats to make a security tour around the ship and give special attention to the waterline and hull. Boats must be identifiable night and day to ship's personnel.

16. Water taxis, ferries, bum boats and other harbor craft require special concern because they can serve as ideal platforms for terrorists. Unauthorized craft should be kept away from the ship; authorized craft should be carefully controlled, surveilled and covered.

17. Identify and inspect workboats.

18. Secure spaces not in use.

19. Regulate shipboard lighting to best meet threat environment. Lighting should include illumination of the waterline.

20. Rig hawsepipe covers and rat guards on all lines, cables and hoses. Consider using an anchor collar.

21. Raise accommodation ladders, stern gates, jacob ladders, etc. when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts and lines.

22. Conduct security drills to include bomb threat and repel boarders exercises.

23. Review individual actions in THREATCON BRAVO for possible implementation.

24. Spare.

c. **THREATCON BRAVO** is declared 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 hardships, affecting operational capability or aggravating relations with local authorities.

25. Maintain appropriate THREATCON ALPHA measures.

26. Review liberty policy in light of the threat and revise it as necessary to maintain safety and security of ship and crew.

27. Conduct divisional quarters at foul weather parade to determine status of on board personnel and disseminate information.

28. Ensure an up-to-date list of bilingual personnel for area of operations. Ensure warning tape in pilot house/quarterdeck that warns small craft to remain clear is in both the local language and English.

29. Remind all personnel to: (a) be suspicious and inquisitive of strangers, particularly those carrying suitcases or other containers; (b) be alert for abandoned parcels or suitcases; (c) be alert for unattended vehicles in the vicinity; (d) be wary of any unusual activities; and (e) notify the OOD of any suspicions.

30. Remind personnel to lock their parked vehicles and check them for signs of tampering before entering.

31. Designate and brief picket boat crews. Prepare boats and place crews on 15 minute alert. If situation warrants, make random picket boat patrols in immediate vicinity of the ship with the motor whaleboat or gig. Boat crews will be armed with rifles, one M60 machine gun with 200 rounds of ammunition and 10 concussion grenades.

32. Consistent with local rules, regulations and Status of Forces Agreement, establish armed brow watch on the pier to check IDs and inspect baggage prior to personnel boarding ship.

33. Man signal bridge or pilot house and ensure flares are available to ward off approaching craft.

34. After working hours, place armed sentries on a superstructure level(s) from which they can best cover areas about the ship.

35. Arm all members of the quarterdeck watch and Security Alert Team (SAT). In the absence of a SAT, arm two members of the SSDF.

36. Provide shotgun and ammunition to quarterdeck. If situation warrants, place sentry with shotgun inside the superstructure at a site from which the quarterdeck can be covered.

37. Issue arms to selected qualified officers to include CDO and ACDO.

38. Arm Sounding and Security Patrol.

39. Muster and brief ammunition bearers/messengers.

40. Implement procedures for expedient issue of firearms and ammunition from Small Arms Locker(s) (SAL). Ensure a set of SAL keys are readily available and in the possession of an officer designated for this duty by the commanding officer.

41. Load additional **small** arms magazine clips to ensure adequate supply for security personnel **and** response forces.

42. **Inform** local authorities of actions being taken as THREATCON increases.

43. Test communications with local authorities and other U.S. Navy ships in port.

44. Instruct watches to conduct frequent random searches under piers, with emphasis on potential hiding places, pier pilings and floating debris.

45. Conduct searches of the ship's hull and boats at intermittent intervals immediately before it puts to sea.

46. Move cars and objects such as crates and trash containers 100 feet from the ship.

47. Hoist boats aboard when not in use.

48. Terminate all public visits.

49. Set material condition YOKE, main deck and below.

50. After working hours, reduce entry points to ship's interior by securing selected entrances from inside.

51. Duty department heads ensure all spaces not in regular us are secured and inspected periodically.

52. Remove one brow if two are rigged.

53. Maintain capability to get underway on short notice as specified by SOPA. Consider possible relocation sites (different pier, anchorage, etc.). Rig brow/accommodation ladder for immediate raising/removal.

54. Ensure .50 caliber machine gun mount assemblies are in place with ammunition in ready service lockers (.50 caliber machine guns themselves will be maintained in the armory, pre-fire checks completed, ready for use).

55. Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats and ultra-light aircraft.

56. Obstruct possible helicopter landing areas in such a manner to prevent hostile helicopters from landing.

57. Review riot/crowd control procedures, asylum seeker procedures and bomb threat procedures.

58. Monitor local communications (ship to ship, TV, radio, police scanners, etc.).

59. Implement additional security measures for high-risk personnel as appropriate.

60. Review individual actions in THREATCON CHARLIE for possible implementation.

61& 62. Spare.

d. **THREATCON CHARLIE** is declared when an incident occurs or intelligence is received indicating that some form of terrorist action against installations and personnel is imminent. Implementation of this threat condition for more than a short period will probably create hardship and affect the peacetime activities of the ship and its personnel.

63. Maintain appropriate THREATCON ALPHA and BRAVO measures.

64. Cancel liberty. Execute emergency recall.

65. Be prepared to get underway on one hour's notice or less. If conditions warrant, request permission to sortie.

66. Call away security alert, deploy Reserve Force to protect command structure and augment posted security watches. In the absence of a Security Alert Force, Backup Alert Force or Reserve Force, muster and arm one squad of the Ship's Self Defense Force.

67. Place armed sentries on a superstructure level(s) from which they can best cover areas about the ship.

68. Establish .50 or .30 caliber machine gun positions.

69. If available, deploy STINGER surface-to-air missiles.

70. Energize radar and establish watch, coordinate with SOPA.

71. Ships with high power sonars operate actively for random periods to deter underwater activity.

72. Man one or more repair lockers. Establish communications with an extra watch in damage control central.

73. Deploy picket boat(s). Boats should be identifiable night and day from ship (e.g., lights or flags).

74. If feasible, deploy helicopter as observation/gun platform. Helicopters should be identifiable night and day from the ship.

75. Activate antiswimmer watch.

76. Issue weapons to other selected officers and chief petty officers in the duty section (commanding officer, executive officer, dept. heads, etc.).

77. Issue concussion grenades to topside rovers, forecastle and fantail sentries and bridge watch.

78. Erect barriers and obstacles as required to control traffic flow.

79. Strictly enforce entry control procedures and inspections.

80. Enforce boat exclusion zone.

81. Minimize all off-ship administrative trips.

82. Discontinue contract work.

83. Set material condition ZEBRA, second deck and below.

84. Secure from inside all unguarded entry points to interior of ship.

85. Rotate screws and cycle rudder(s) at frequent and irregular intervals.

86. Rig additional firehoses. Firehoses will be charged when manned just prior to actual use.

87. Review individual actions in THREATCON DELTA for implementation.

88. Spare.

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

89. Maintain appropriate THREATCON ALPHA, BRAVO and CHARLIE measures.

90. Permit only necessary personnel topside.

91. Prepare to get underway and, if possible, cancel port visit and depart.

92. Post sentries with M60 machine gun(s) to cover possible helicopter landing areas.

93. Arm selected personnel of SSDF.

94. Deploy grenade launchers to cover approaches to ship.

95. Spare.

PRE-PORT ARRIVAL PROCEDURES FOR AFLOAT UNITS

1. Review ship's mission, reason for port visit, and duration of visit.

2. Review NCIS threat assessment, Navy Blue Dart Messages, NAVATAC Spot Reports, NAVATAC daily summaries and any other intelligence information available.

3. Obtain/review other agreements in effect. If necessary, send message to responsible MAAG/Mission or Consulate requesting information.

   a. Jurisdiction.
   b. Arming of topside and other watchstanders.
   c. Host country emergency support availability and how to contact.

4. Will ship be alongside a shore structure (pier, wharf, or quay) or anchored? (Following information may be included in a port visit request message.

   a. If alongside a shore structure:

      (1) Is area U.S. or foreign controlled? Ascertain jurisdiction and lines of responsibility.
      (2) Will pier watches be military, civilian or both? If civilian, will the forces be standard police forces or hired guards?
      (3) Height of pier. Number of camels to be requested and/or other ability to breast out, if brows can support the span.
      (4) "Normal" pier traffic expected.

   b. If anchored:

      (1) Availability of foreign waterborne support (e.g., host Coast Guard and/or naval units).
      (2) Review possibility of own-ship picket boat operations. Include:
         a. Legal ramifications.
         b. Logistics capabilities (suitable boat, boat crew training, etc.)
      (3) Normal traffic through the expected anchorage area.
      (4) Whether anchorage is in a tidal flow or still water (affects floating bombs, mines and swimmers). Obtain times and strength of tidal changes.

5. Review ship's watchstander qualifications and posting.

6. Review SSDF qualifications and training.

7. Conduct general AT/FP training, include AT awareness specific items in In-port brief.

PRE- ARRIVAL PROCEDURES FOR AIRCREWS

1. Review mission, reason and duration of visit.

2. Prior to flight:

   a. Review NCIS threat assessment, Navy Blue Dart Messages, NAVATAC Spot Reports, NAVATAC daily summaries and any other intelligence information available.

   b. Obtain/review SOFAs/other agreements in effect. If necessary, send message to responsible MAAG/Mission or Consulate requesting information.

   c. Ascertain jurisdiction.

   d. Address availability of hangars, secure aircraft holding areas, and availability of armed guards. Determine whether guards are U.S., host police, contract guards or host military.

   e. Address requirement for country clearance, including surrounding country overflight requirements.

   f. Conduct general AT/FP training, include awareness specific items in Departure/Pre-Flight briefing.

3. Upon arrival, determine host country emergency support availability and how to contact.

4. Identify secure transportation arrangements for the crew from and to the aircraft holding areas.

5. Identify most secure berthing arrangements for the crew (if staying overnight).

PRE-ARRIVAL PROCEDURES FOR SMALL COMMAND OICs

1. Review mission, reason and duration of visit.

2. Prior to travel:

a. Review NCIS threat assessment, Navy Blue Dart Messages, NAVATAC Spot Reports, NAVATAC daily summaries and other intelligence information available.

b. Obtain/review SOFAs/other agreements in effect (if applicable). If necessary, send message to responsible MAAG/Mission or Consulate requesting information.

d. Requirement for country clearance, including surrounding country overflight requirements.

e. Conduct general AT/FP training, include AT awareness specific items in In-port brief.

3. Upon arrival, determine host country emergency support availability and how to contact.

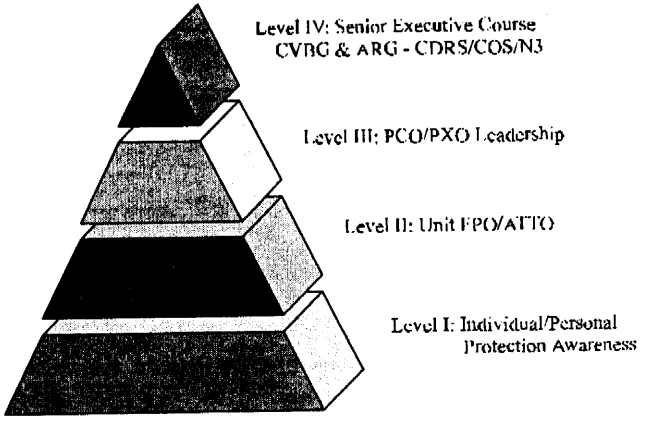
4. Identify in-country transportation arrangements. If transportation is not provided, requirement for international drivers licences.

5. Identify most secure berthing arrangements.

TRAINING

"DoD Combating Terrorism Program Procedures," requires AT threat awareness and personal protection training in all officer and enlisted initial entry training. Basic branch qualification courses will then train this task to more specific, branch or occupation related functions. NCO leadership, officer staff and command, and joint schools will conduct training and exercises designed to integrate staff functions for combating terrorism.

Unit-Level Training. Services are tasked with providing training on terrorist threat and personnel protection principles and techniques; instituting awareness programs designed to raise the awareness of Service personnel and their family members to the general terrorist threat; and teaching measures that reduce personal vulnerability. CINCs are charged with developing and maintaining an Antiterrorism program, identifying AOR specific antiterrorism training requirements for personnel prior to arrival, and conducting field or staff training at least annually to exercise AT plans.



NAVY IG SPECIAL INTEREST ITEM: ANTITERRORISM READINESS

COMBATING TERRORISM (ANTITERRORISM/COUNTERTERRORISM)

1. Does the orgnaization have a combating terrorism program in accordance with DoDD 2000.12 and/or Service implementing document?

2. Does the organization have a combating terrorism plan IAW DODD 2000.12 and/or Service implementing document?

3. Is antiterrorism (AT) planning integrated into overall force protection planning as recommended by DoD 2000.12-H?

4. Has the combating terrorism plan been coordinted with foreign, state and local law enforcement agencies as recommended by DoD 2000.12-H?

ANTITERRORISM PLANNING AND OPERATIONS

5. Does the organization have the most current version of all appropriate directives, instructions, regulations and other pertinent documents?

6. Has the organization designated an antiterrorism officer and provided for their training IAW DODINST 2000.14 and/or the Service implementing document?

7. Has the organization established an AT awareness program IAW DODD 2000.12?

8. Do all members of the organization receive periodic terrorism awareness briefings IAW DODD 2000.12?

9. Has the organization conducted an AT exercise within the last 12 monsts IAW DODINST 2000.14 and/or Service implementing documents?

10. Have terrorism scenarios been integrated into training exercises IAW DODINST 2000.14 and/or the Service implementing documents?

11. Has the organization performed either a vulnerability assessment or a risk analysis as recommended by DoD 2000.12-H?

12. a) Has a prioritized list of Mission Essential Vulnerable Areas been established as recommended by DoD 2000.12-H and Service guidance?
b) Is there a plan of action and have milestones been established for addressing vulnerable areas?

13. a) Does the organization have a crisis management team as recommended by DoD 2000.12-H?
b) Does it have proper staff representation and has it met within the last 90 days?
c) Has the organization followed guidance of DoD 2000.12-H, Chapter 15, "Terrorism Crisis Management Planning and Execution?"

ANTITERRORISM FOR UNIT DEPLOYMENTS

14. a) Are there well-defined and located specific pre-deployment AT requirements as recommended by DoD 2000.12-H and Joint Pub 3-07.2?
b) Do they provide for pre-deployment threat awareness training?
c) Do they identify key elements for additional protection after deployment?
d) Do they ensure against interruption of the flow of threat information to deployed units?

THREAT INFORMATION: COLLECTION AND DISSEMINATION

15. Do procedures exist to allow for the timely dissemination of terrorist threat both during and after duty hours IAW DODD 2000.12?

16. Does the organization have a travel security program and does it provide threat information briefings on a regular basis IAW DODD 2000.12?

17. a) Has collection and dissemination of terrorist information been reviewed by the Commander in the last year?
b) Did the Commanding Officer assess it as adequate?

18. Is the threat assessment current IAW DODD 2000.12?

19. Does the organization receive recurring threat updates IAW DODD 2000.12 and/or the Service implementing document?

20. Is the intelligence analysis at the installation of deployed location a blend of all appropriate intelligence disciplines and does the intelligence officer understand the sources of the information?

21. Are there indications that all available information is not being collected?

PHISICAL SECURITY

22. Does the organization have a physical security plan IAW DODD 2000.12 and DODD 5200.8?

23. Are AT protective measures incorporated into the physical security plan as recommended by DOD 2000.12-H?

24. Have procedures been established to ensure that all military construction projects are reviewed at the conceptual stage to incorporate physical security, antiterrorist or protective design features IAW DODD 5200.8-R?

LAW ENFORCEMENT AGENCY INVOLVEMENT

25. Is Law Enforcement Agency developed information shared and blended with Intelligence information as recommended by DOD 2000.12-H?

26. Is there a mutual understanding between all local agencies that might be involved in a terrorist incident on the installation regarding authority, jurisdiction and possible intteraction as recommended by DOD 2000.12-H?

FUNDING

27. Were AT funding requirements identified during the POM cycle? Please provide the detailed information involved in the POM submission.

28. Have required AT enhancements been identified and prioritized?

29. Are there shortfalls in AT funding projected in FY XXXX? If so, what are they?

30. a) What percentage of requested funding was received in FY XXXX [previous FY]?
    b) Amount requested? $
    c) Amount received? $

31. Has the lack of funding adversely impacted the organization's AT program? If yes, please comment.

REFERENCES:

DODD 2000.12:	"DOD Combating Terrorist Program," September 15, 1996
DOD 2000.12-H:	"Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February 1993
DODINST 2000.14:	"DOD Combatting Terrorism Program Procedures," June 1994
DODD 5200.8:	"Security of Military Installations and Resources," April 1991
DODD 5200.8-R:	"Physical Security Program," May 1991
Joint Pub 3-07.2:	"Joint Tactics, Techniques and Procedures (JTTP) Antiterrorism," June 25, 1993

For copies of this document please contact JO1(SW) Priscilla Kirsh, N09N3/NCIS-24J at (202) 433-9096 DSN 288-9096. E-Mail PKIRSH@cs27.frodo.org

EMERGENCY PHONE NUMBERS

NCIS _____

FBI _____

Unit Force Protection Officer _____

Unit AT Awareness Training Officer _____

Security _____

Police _____

Fire _____

Medical _____

Explosive Ordnance _____

Navy Organizations responsible for Antiterrorism/Force Protection

CNO/N312
Current Joint Operations and Plans Branch
Room 4D600
2000 Navy Pentagon
Washington, DC 20350
(703) 697-6033/5641
(703) 695-1150/1151 (DSN 227)
Fax: 703-695-8518
DSN 225-8518

CNO/N09N3/NCIS-24
Deputy Assistant Director for
Law Enforcement and Physical Security Programs
Code 24
Naval Criminal Investigative Service Headquarters
Bldg. 111 901 M Street SE
Washington, DC 20388
Phone: 202-433-9077 (DSN 288) Fax: 202-433-9147

Navy Antiterrorist Alert Center
Naval Criminal Investigative Service Headquarters
Bldg. 111 901 M Street SE
Washington, DC 20388
Phone 202-433-9418/19/90
Fax: 202-433-9434/9390

Although not all inclusive, this guide should serve as a tool to assist commanders in creating an environment in which the lives and well-being of our Sailors and families are an integral part of the accomplishment of our mission.