

the responsibility of all commanders to ensure the full participation of everyone in their unit in the AT program. However, no single installation can provide a complete AT posture without the aid of outside resources and tenant command support. This agreement will mitigate many of the vulnerabilities that exist before an actual crisis, either natural or manmade, as well as aid in the post-incident response to a crisis.

3. Scope. This MOA will remain in effect until written notice by either signatory, at which time it will be reviewed and updated. Each signatory reserves the right to request review and modification of the MOA should changes to the table of organization (T/O) or table of equipment (T/E), mission, or other circumstances warrant revision.

4. Assumptions

a. Individual installation Commanding Officers subordinate to the Commanding General, Marine Corps Installations, and establish the FPCON for their installation based on threats and the risks of other natural or manmade hazards. Subordinate commanders may raise a FPCON, as directed by a higher level commander, for those personnel and assets for which they have AT responsibilities. Subordinate commanders will not lower a higher-level commander's FPCON without concurrence. The duration of a heightened FPCON is scenario-dependent.

b. The amount and type of MEF support to Marine Corps installations required will be determined on a case-by-case basis. Every effort will be made to provide installations with their requested support and to minimize the operational impact on MEF tenant units.

5. Responsibilities

a. Commanding General, Marine Corps Installations

(1) Direct Installation Commanding Officers to notify the senior MEF tenant command Commanding Officers aboard their installations, anytime a Marine Corps Installation Commander's Critical Information Requirements (CCIR) has been triggered. This will occur during working and non-working hours.

(2) Direct Installation Commanders to coordinate with tenant MEF forces to develop plans designed to respond to, and

mitigate, local area disasters, both manmade and naturally occurring. These efforts should be established in conjunction with existing tactics, techniques, and procedures (TTPs), as well as the installations' AT plans.

(3) Direct installations to forward threat information or suspicious incidents, listed in enclosure (1) to the Installation Information Fusion Cell (IFC), as well as MEF Current Operations for analysis. Unclassified threat information may be forwarded to the IFC via the Installation Command Duty Officer (CDO) at emailaddress@usmc.mil or by phone at (XXX) XXX-XXXX (duty hours) or (XXX) XXX-XXXX (off duty hours). The MEF Senior Watch Officer (SWO) may be contacted at emailaddress@usmc.mil or by phone at (XXX) XXX-XXXX. Classified threat information may be forwarded via by phone at (XXX) XXX-XXXX (STU III) or emailaddress@usmc.mil.

(4) Direct subordinate installation Commanding Officers to convene a Threat Working Group (TWG) when in receipt of Indications and Warnings (I&W) or terrorist threat information. Ensure the TWG includes a representative of the senior Commanding Officer subordinate to MEF that is aboard their installation.

b. Commanding General, Marine Expeditionary Force

(1) Direct the MEF SWO to take appropriate action on threat information and provide timely feedback to Marine Corps installation for support from MEF units.

(2) Direct the MEF SWO to track and update the MEF Commanding General on any crisis situation aboard Marine Corps installations, including support being provided by MEF units.

(3) Coordinate with Marine Corps installation and its subordinate installations to establish local MOAs that will determine the appropriate size and makeup of the respective Security Augmentation Forces (SAF).

(4) Direct MEF units that require on-base armed Guardian Angel support to coordinate with their local Provost Marshal's Office as soon as possible, before the event.

(5) Identify a MEF Liaison Officer (LNO) per each Marine Corps installation base and station, to include Marine Corps installation headquarters, to provide a direct link to the

MEF SWO during times when the base or station Command Operations Center/Emergency Operations Center (COC/EOC) is activated.

(6) Providing FP for all in-transit forces will be the responsibility of MEF. MEF will notify Marine Corps installation CDO of any required, non-standard, support requirements.

(7) Be prepared to provide resources, as available, that are not listed in this MOA that may be requested for incident response.

(8) Provide assistance, as resources are available, to the Marine Corps installation IFC for information analysis and information fusion.

(9) Forward all threat information and/or I&W information to the Marine Corps installation IFC for review and dissemination.

(10) Identify the MEF senior tenant Commanding Officer aboard each Marine Corps installation who is to be notified in the event a Marine Corps Installation Commander's CCIR has been tripped. Once a Marine Corps installation Commander's CCIR has been tripped, the MEF senior tenant Commanding Officer will notify the other MEF Commanding Officers aboard their installation, as well as the MEF SWO immediately upon notification.

6. End State. Marine Corps installation, along with support from MEF forces, will provide a robust FP capability and in the event respond to any threat situation (manmade or natural) rapidly and efficiently.

7. Effective Date. This MOA is effective upon receipt.

JOHN SMITH

JOHN DOE

ENCLOSURE (1) TO MEMORANDUM OF AGREEMENT (MOA) FOR EMERGENCY NOTIFICATION, INFORMATION SHARING, SECURITY AUGMENTATION, AND MEF SUPPORT TO MARINE CORPS INSTALLATION BASES AND STATIONS DURING A CRISIS EVENT: THREAT INFORMATION MANAGEMENT

1. **General**

a. **Purpose.** Establish procedures for threat information management. Threat information management in this instance equates to the use of the information fusion process to expeditiously report salient suspicious activity potentially affecting Marine Corps installation bases and stations

b. **Mission.** Marine Corps Installation, in coordination with MEF, collaboratively manage and disseminate threat information to prepare for, respond to, or recover from natural or manmade disasters affecting or potentially affecting Marine Corps Installation or MEF operations.

c. **Situation.** Information fusion facilitates preparing for, responding to, or recovering from all hazards whether natural or manmade. Threat information management is primarily achieved through the information fusion process which consists of analyzing and conducting trend analysis of any threat information received by Marine Corps Installation and/or MEF. This information is subsequently disseminated in a consolidated, useful format to all concerned to synchronize all-hazard preparation/response/recovery and promote individual awareness. Marine Corps Installation and MEF possess varying levels of capability. Significant synergy regarding information fusion is achievable if both commands collaboratively work toward this common goal.

2. **Reportable Criteria.**

a. **CCIRs.** Per MOA.

b. **Specific Threats.** Any threat received by any means that contains a specific time and location for an attack against U.S. Forces, facilities, or missions in the geographic area. Examples include: any event or incident, or series of events, which in and of themselves overwhelmingly indicate a threat to U.S. Forces, facilities, or mission.

c. **Ambiguous Threats.** Non-specific threats received by any means that do not necessarily specify a time or location for an attack but when considered in conjunction with other information and/or experience dictate credibility.

d. **Surveillance.** Acts of surveillance from outside sources or from within the installation that are deliberate and/or clandestine, which attempt to record sensitive operational, electronic, or security related information by any means (e.g., cameras, direct observation, vision-enhancing devices, cyber eavesdropping or attack, etc.).

e. **Compromise or Possible Compromise of Classified or Personal Identification Information.** Examples include any inadvertent loss or unauthorized acquisition of or attempt to acquire classified or personal identification (e.g., addresses, SSNs, phone numbers, etc.) information by any means.

f. **Suspicious Activity.** Any activity that appears threateningly odd or out of place, especially when considered in conjunction with other known threat information and/or experience.

3. **Reporting Channels.**

a. Use the chain of command except when the situation dictates (e.g., immediate threat to life) it is clearly inexpedient to do so. If the latter is the case, dial 9-1-1, and then notify the chain of command.

b. The Marine Corps Installation CDO, Marine Corps Installation Threat Information Manager, MEF SWO, and installation PMO must be notified as soon after the activity or incident as possible. The success of threat information reporting can be measured in the expedient and efficient transfer of information.

OFFICIAL:

JOHN SMITH

JOHN DOE

APPENDIX E

SAMPLE FPCON ACTION SETS

<u>FPCON ALPHA</u>	<u>Marine Corps Base Actions</u>
<p>FPCON ALPHA applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. ALPHA measures must be capable of being maintained indefinitely.</p>	<p><u>CO</u>: Convene CMT and develop courses of actions. This planning session should consider implementation of higher FPCONs.</p> <p><u>All Units</u>:</p> <p>Complete all required actions for previous FPCONs.</p> <p>Complete all required actions for FPCON ALPHA</p> <p>Report actions complete to Operations.</p> <p><u>Be prepared to implement higher FPCONs.</u></p>
<p><u>Measure ALPHA 1.</u> Continue, or introduce, all measures in previous FPCON.</p> <p>Critical Infrastructure Protection (CIP) Measure.</p>	<p><u>AT Div</u>: Ensure PMO conducts Crime Prevention briefs, as appropriate.</p> <p><u>Critical Asset Owners</u>: Regularly brief personnel on operational security procedures and review Emergency Action Plans. Periodically conduct refresher training for disaster response. Regularly test internal procedures, generators, communication/cyber systems, etc.</p>
<p><u>Measure ALPHA 2.</u> At regular intervals, inform personnel and family members of the general situation. Ensure</p>	<p><u>Manpower</u>: Conduct suspicious packages/IED training for all mail handlers.</p>

<p>personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.</p>	<p><u>AT Div:</u> Coordinate Eagle Eye and America's Waterway Watch Programs.</p> <p><u>PAO:</u> Remind personnel, via various media outlets, to report suspicious activity to 911. Prepare public information media release templates for various AT threat scenarios.</p> <p><u>All Units:</u> Regularly brief all personnel on the current terrorist threat as part of the Troop Information Program.</p> <p>Ensure personnel receive Annual Level I AT Awareness training.</p>
<p><u>Measure ALPHA 3.</u> The duty officer or personnel with access to building plans, as well as the plans for area evacuations, must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on call and readily available.</p>	<p><u>DPS:</u> Ensure key personnel required to implement security plans are on call and readily available.</p> <p>Ensure recall rosters are current.</p> <p><u>PMO:</u> Review and update access control procedures as required.</p> <p><u>Manpower:</u> Ensure CDOs have a copy of this AT Plan and are familiar with its implementation.</p> <p>Ensure recall rosters are current.</p> <p><u>S-4:</u> Maintain building schematics and be prepared to provide them upon request.</p> <p>Coordinate with appropriate department for on-call heavy equipment operators.</p> <p><u>Area Cmdrs:</u> Institute and rehearse recall procedures and monitor status of interior guard and security</p>

<p>Critical Infrastructure Protection (CIP) Measure.</p>	<p>augmentation forces.</p> <p>All Units: Ensure emergency personnel recall rosters are current. Familiarize all personnel with building evacuation plans.</p> <p>Bldg Managers: Ensure building/unit bomb threat plans and physical security orders are current. Revise/exercise evacuation plans as appropriate.</p> <p>Critical Asset Owners: Ensure emergency personnel recall rosters are current. Review bomb threat and building evacuation plans.</p>
<p>Measure ALPHA 4. Increase security spot checks of vehicles and persons entering the Installation under the jurisdiction of the United States.</p>	<p>PMO: Increase random identification spot checks of passenger and commercial vehicle occupants entering the Base including pedestrians, joggers, and bicyclists.</p> <p>Conduct DoD decal monitoring.</p> <p>Increase random vehicle inspections at various locations on the Base. Incorporate the use of explosive and narcotic detection dogs.</p> <p>Verify commercial deliveries by checking the driver's ID and bill of lading.</p> <p>Coordinate potential traffic congestion problems with law enforcement and emergency management agencies.</p> <p>S-4/S-6/MCCS/Commissary/DoD Schools: Inform vendors to use the commercial vehicle gate and that delivery personnel must present a picture ID and a bill of lading before being</p>

<p>Critical Infrastructure Protection (CIP) Measure.</p>	<p>allowed access to the Base. Be prepared to validate/verify that the vendor is authorized aboard the Base. Ensure that ID card check of patrons is continually applied.</p> <p><u>CMDRS/All Units:</u></p> <p>Ensure POVs are properly registered.</p> <p>Ensure all personnel have ID cards.</p> <p><u>Critical Asset Owners:</u> Strictly enforce POV parking policy and vehicle standoff distances.</p>
<p>Measure ALPHA 5. Initiate food and water Operational Risk Management (ORM) procedures, brief personnel on food and water security procedures, and report any unusual activities.</p> <p>Critical Infrastructure Protection (CIP) Measure.</p>	<p><u>S-4/MCCS/Commissary:</u> Brief personnel to monitor food deliveries and report activities that do not appear to be normal, such as change of delivery personnel and open packages/containers.</p> <p><u>PAO:</u> Provide media coverage to brief the public on food and water security procedures and the reporting of suspicious activities.</p> <p><u>Managers/Supervisors of Water Treatment Facilities:</u> Brief personnel on water security procedures and the reporting of suspicious activities.</p>
<p><u>FPCON DELTA</u></p>	<p><u>Marine Corps Base Actions</u></p>
<p>FPCON 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 imminent. Normally, this FPCON is declared as a localized condition. FPCON</p>	<p><u>CO:</u> Request activation of the MOU between the Commander, Department of Homeland Security/U.S. Coast Guard Sector to establish a temporary security zone.</p> <p>Request activation of the Security Augmentation Force (SAF).</p>

<p>Delta measures are not intended to be sustained for substantial periods.</p>	
<p><u>Measure DELTA 1.</u> Fully implement all measures of lower FPCONs Levels.</p>	<p><u>All Units:</u> Complete all required actions for previous FPCONs.</p> <p><u>CO:</u> Convene the CMT.</p> <p>Review actions taken for lower FPCONs.</p> <p>Suspend all military training.</p> <p>Close all non-essential MCCS/Commissary/Base services.</p> <p>Send all non-essential personnel home.</p> <p>Suspend DoD schools.</p> <p>Keep personnel and local governments informed.</p> <p>Evaluate courses of action to return to a lower FPCON.</p> <p><u>Dir/Area/Tenant Cmdrs/Bldg Managers:</u> Review actions taken and amend as required.</p>
<p><u>Measure DELTA 2.</u> Augment guards as necessary.</p>	<ul style="list-style-type: none"> • <u>PMO:</u> Assume command and control of the Security Augmentation Force (SAF). • • <u>Dir/Area/Tenant Cmdrs:</u> • Report additional security requirements to the Base EOC. <p><u>CMT:</u> Prioritize additional security requirements.</p>
<p><u>Measure DELTA 3.</u> Identify all vehicles within operational or</p>	<p><u>ISS-PMO:</u> Conduct record checks on suspicious/unattended vehicle around</p>

<p>mission support areas.</p>	<p>Critical Assets, potential terrorist targets, and other "soft targets."</p> <p>Conduct random checks to ensure compliance.</p> <p><u>Dirs/Area/Tenant Cmdrs:</u> Assist PMO in identifying suspicious/unattended vehicles. Report vehicles to the Base EOC for coordination of records check.</p>
<p><u>Measure DELTA 4.</u> Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles use to transport escorted Very Important Personnel (VIPs) maybe exempted.</p>	<p><u>PMO:</u> Institute 100% vehicle searches at gates and notify cooperating federal and military agencies of requirement. Coordinate with the State Highway Patrol, Police Department and Sheriff's Office, as required.</p> <p><u>PAO:</u> Notify the public accordingly.</p> <p><u>All Dirs/Area/Tenant Cmdrs:</u> Instruct personnel to keep traffic into the Base to an absolute minimum.</p>
<p><u>Measure DELTA 5.</u> Control facility access and implement positive identification of all personnel with no exceptions.</p>	<p><u>PMO:</u> Continue 100% ID checks at all gates.</p> <p><u>Dirs/Area/Tenant Cmdrs:</u> Establish access rosters and institute 100% ID checks at all facilities. Restrict access to critical assets to mission-essential personnel only.</p>

APPENDIX F

SAMPLE FPCON CHANGE REPORT

TO: (GEOGRAPHIC COMBATANT COMMANDER) (UC)
CMC WASHINGTON DC PPO PS (UC)

CC: (CHAIN OF COMMAND) (UC)

UNCLAS//FOUO

SUBJ: FPCON (ELEVATION/CHANGE) AT (STATION/FACILITY) TO FPCON
(ALPHA/BRAVO/CHARLIE/DELTA) .//

REF/A/GCC PROVIDES GUIDANCE FOR REPORTING FPCON CHANGES IE.
(USNORTHCOM AT OPORD/DTD 15JUL06))//

AMPN/REF A DIRECTS FPCON CHANGE NOTIFICATION WITHIN 4 HOURS OF
CHANGE.//

MSGID/FPCON CHANGE REPORT/COMMARFORNORTH/G3/ATFP//

POC/ATO RELEASING MESSAGE)//

REMARKS/1. (U/FOUO) AFFECTED (GCC) ELEMENT:

1.A. (U/FOUO) NEW FPCON LEVEL:

1.B. (U/FOUO) DTG EFFECTIVE:

1.C. (U/FOUO) WHY:

1.D. (U/FOUO) WHO DIRECTED:

1.E. (U/FOUO) DURATION OF CHANGE:

2. (ADDITIONAL DETAILS, AS REQUIRED)//

BT

NNNN

APPENDIX G

SAMPLE RAM PROGRAM

This Sample RAM Program provides a detailed schedule for RAM implementation. After the PMO develops the various RAM sets, the ATO approves and schedules the RAM sets. Robust RAM Programs typically have between five and eight sets of RAMs. However, this sample RAM Program only provides two example sets. Additional RAM sets can be developed by changing the time or measure. RAMs may be color coded in order to more easily identify certain categories, such as usage of MWDs, ID checks, building checks, etc. Once the RAM sets have been developed, ATOs should create a yearly calendar outlining when each RAM set should be implemented. The Sample RAM Schedule shows the random employment of seven RAM sets.

RAM SET #1

MARINE CORPS BASE XYZ Weekly RAM Report

The following RAMs are submitted for approval in order to give the MCB XYZ visibility of high profile AT security measures performed by MCB XYZ. These measures are in addition to other RAMs performed on a routine basis that are unscheduled. These measures will be captured daily in the MPD Desk Journal.

THE CURRENT FPCON IS ALPHA

The following RAMs will be implemented at MCB XYZ.

SATURDAY

0500-0800 100% ID CARD CHECKS AT MAIN GATE
0540-0740 SHOTGUN OVER WATCH AT BACK GATE (MEASURE 37)
0700-0900 100% ID CARD CHECKS AT BACK GATE
1005-1135 MWD XYZ PERIMETER PATROLS
1500-1600 100% ID CARD CHECKS AT BACK GATE
1515-1615 RANDOM ID CHECKS AT XYZ ANNEX (MEASURE 13)
1550-1750 100% ID CARD CHECKS AT MAIN GATE

SUNDAY

0715-0815 SRT, AID, MWD DUTY CELLULAR PHONE AND PAGER CHECKS (MEASURE 21)
1100-1300 100% ID CARD CHECKS AT BACK GATE
1245-1345 MWD PRESENCE AT MAIN GATE (MEASURE 30)
1245-1345 RANDOM VEHICLE INSPECTIONS AT MAIN GATE (MEASURE 1)
1300-1500 100% ID CARD CHECKS AT MAIN GATE
1800-1900 100% ID CARD CHECKS AT BACK GATE
2100-0000 100% ID CARD CHECKS AT MAIN GATE

MONDAY

0000-0200 100% ID CARD CHECKS AT MAIN GATE
0110-0310 PERIMETER PATROLS OF FENCE LINE (MEASURE 12)
0530-0630 100% ID CARD CHECKS AT BACK GATE
1015-1115 WALKING PATROLS AT COMMISSARY (MEASURE 41)
1110-1410 100% ID CARD CHECKS AT MAIN GATE
1505-1635 RANDOM VEHICLE INSPECTIONS AT BACK GATE WITH UNDER
VEHICLE INSPECTIONS SYSTEM (MEASURE 1A)
1900-2100 100% ID CARD CHECKS AT BACK GATE

TUESDAY

0240-0440 100% ID CARD CHECKS AT MAIN GATE
0835-0935 MWD PRESENCE AT MAIN GATE (MEASURE 30)
0835-0935 COMMERCIAL VEHICLE INSPECTIONS AT MAIN GATE (MEASURE
5)
0900-1100 100% ID CARD CHECKS AT BACK GATE
1300-1400 100% ID CARD CHECKS AT BACK GATE
1500-1800 100% ID CARD CHECKS AT MAIN GATE
1705-1805 WALKING PATROLS OF COMMISSARY (MEASURE 41)

WEDNESDAY

0400-0600 100% ID CARD CHECKS AT MAIN GATE
0600-0700 100% ID CARD CHECKS AT BACK GATE
0635-0735 SHOTGUN OVER WATCH AT MAIN GATE (MEASURE 37)
1510-1610 MWD PRESENCE AT MAIN GATE (MEASURE 30)
1510-1610 COMMERCIAL VEHICLE INSPECTIONS AT MAIN GATE (MEASURE
5)
2000-2200 100% ID CARD CHECKS AT BACK GATE
2045-2345 100% ID CARD CHECKS AT MAIN GATE

THURSDAY

0630-0830 100% ID CARD CHECKS AT MAIN GATE
0725-0825 WALKING PATROL CONDUCTED AT ELEMENTARY SCHOOL (MEASURE
40) (NOTE CANCEL WHEN SCHOOL IS NOT IN SESSION)
0920-1050 RANDOM VEHICLE INSPECTIONS AT MAIN GATE WITH UNDER
VEHICLE INSPECTION SYSTEM (MEASURE 1A)
1000-1100 100% ID CARD CHECKS AT BACK GATE
1320-1450 MWD FLIGHTLINE PATROLS
1600-1800 100% ID CARD CHECKS AT BACK GATE
1620-1750 WALKING PATROLS OF MARINE CORPS EXCHANGE (MEASURE 13)
1800-2100 100% ID CARD CHECKS AT MAIN GATE

FRIDAY

0700-0900 100% ID CARD CHECKS AT MAIN GATE
0735-0835 RANDOM PACKAGE CHECKS AT POST OFFICE (MEASURE 20)

1235-1405 WALKING PATROLS OF MARINE CORPS EXCHANGE (MEASURE 41)
1400-1500 100% ID CARD CHECKS AT BACK GATE
1525-1625 PATROL SHORELINE FOR UNAUTHORIZED PERSONNEL (MEASURE
32)
1600-1900 100% ID CARD CHECKS AT MAIN GATE
1800-2000 100% ID CARD CHECKS AT BACK GATE

MCB XYZ RAM totals:

CAT 1 RAMS (MWD EMPLOYMENT): 10 HOURS
CAT 2 RAMS (RANDOM VEHICLE INSPECTIONS): 9 HOURS
CAT 3 RAMS (PERSONNEL INSPECTIONS / ID CHECKS): 135 HOURS
CAT 4 RAMS (ADDITIONAL RAMS): 21 HOURS

RAM SET #2

MARINE CORPS BASE XYZ Weekly RAM Report

The following RAMs are submitted for approval in order to give the MCB XYZ visibility of high profile AT security measures performed by MCB XYZ. These measures are in addition to other RAMs performed on a routine basis that are unscheduled. These measures will be captured daily in the MPD Desk Journal.

THE CURRENT FPCON IS ALPHA

The following RAMs will be implemented by MCB XYZ.

SATURDAY

0000-0200 100% ID CARD CHECKS AT MAIN GATE
0415-0615 100% ID CARD CHECKS AT MAIN GATE
0815-1215 100% ID CARD CHECKS AT BACK GATE
0915-1015 RANDOM PATROL OF FLIGHT LINE RESTRICTED AREA (MEASURE
3)
1300-1500 100% ID CARD CHECKS AT MAIN GATE
1325-1525 SHOTGUN OVER WATCH AT MAIN GATE (MEASURE 37)
1610-1710 MWD PRESENCE AT BACK GATE (MEASURE 30)
1610-1710 RANDOM VEHICLE INSPECTIONS AT BACK GATE (MEASURE 1)
1700-2000 100% ID CARD CHECKS AT BACK GATE
2100-0000 100% ID CARD CHECKS AT MAIN GATE

SUNDAY

0530-0700 100% ID CARD CHECKS AT BACK GATE
0600-0800 100% ID CARD CHECKS AT MAIN GATE
0615-0815 RANDOM VEHICLE INSPECTIONS AT MAIN GATE WITH UNDER
VEHICLE INSPECTION SYSTEM (MEASURE 1A)
1030-1330 100% ID CARD CHECKS AT MAIN GATE
1015-1115 MWD PATROLS OF COMMISSARY (MEASURE 39)

1330-1630 100% ID CARD CHECKS AT BACK GATE
1525-1625 WALKING PATROLS AT MARINE CORPS EXCHANGE (MEASURE 41)
1800-2200 100% ID CARD CHECKS AT MAIN GATE
2000-2200 100% ID CARD CHECKS AT BACK GATE

MONDAY

0215-0615 100% ID CARD CHECKS AT MAIN GATE
0800-1000 100% ID CARD CHECKS AT MAIN GATE
0800-1000 100% ID CARD CHECKS AT BACK GATE
0945-1045 RANDOM ID CHECKS AT MCX ANNEX (MEASURE 13)
1200-1400 100% ID CARD CHECKS AT BACK GATE
1305-1505 COMMERCIAL VEHICLE INSPECTIONS AT MAIN GATE (MEASURE
10)
1305-1505 MWD PRESENCE AT MAIN GATE (MEASURE 30)
1600-1900 100% ID CARD CHECKS AT MAIN GATE
1700-2000 100% ID CARD CHECKS AT BACK GATE

TUESDAY

0000-0200 100% ID CARD CHECKS AT MAIN GATE
0025-0125 SHOTGUN OVER WATCH AT MAIN GATE (MEASURE 37)
0500-0700 100% ID CARD CHECKS AT MAIN GATE
0530-0730 100% ID CARD CHECKS AT BACK GATE
1150-1250 RANDOM VEHICLE INSPECTIONS AT BACK GATE WITH UNDER
VEHICLE INSPECTION SYSTEM (MEASURE 1A)
1350-1450 MWD PATROLS OF MARINE CORPS EXCHANGE (MEASURE 39)
1400-1600 100% ID CARD CHECKS AT BACK GATE
1430-1630 100% ID CARD CHECKS AT MAIN GATE
2100-0000 100% ID CARD CHECKS AT MAIN GATE
2100-2200 100% ID CARD CHECKS AT BACK GATE

WEDNESDAY

0200-0400 100% ID CARD CHECKS AT MAIN GATE
0340-0440 RANDOM PATROL OF FLIGHT LINE RESTRICTED AREA (MEASURE
3)
0700-0900 100% ID CARD CHECKS AT MAIN GATE
0720-0820 WALKING PATROLS AROUND ELEMENTARY SCHOOL (MEASURE 40)
1045-1245 100% ID CARD CHECKS AT BACK GATE
1200-1400 100% ID CARD CHECKS AT MAIN GATE
1210-1310 WALKING PATROLS AT MCX MEASURE 41)
1700-2100 100% ID CARD CHECKS AT BACK GATE
1745-1945 100% ID CARD CHECKS AT MAIN GATE
2235-2335 MWD PATROLS OF CAMP XYZ PERIMETER FENCE LINE (MEASURE
12)

THURSDAY

0400-0700 100% ID CARD CHECKS AT MAIN GATE

0700-1000 100% ID CARD CHECKS AT BACK GATE
0910-1010 MWD PRESENCE AT BACK GATE (MEASURE 30)
0910-1010 COMMERCIAL VEHICLE INSPECTIONS AT BACK GATE (MEASURE
5)
1330-1630 100% ID CARD CHECKS AT BACK GATE
1415-1615 100% ID CARD CHECKS AT MAIN GATE
2100-0000 100% ID CARD CHECKS AT MAIN GATE
2100-2200 100% ID CARD CHECKS AT BACK GATE

FRIDAY

0100-0300 100% ID CARD CHECKS AT MAIN GATE
0155-0355 SHOTGUN OVER WATCH AT MAIN GATE (MEASURE 37)
0530-0600 100% ID CARD CHECKS AT BACK GATE
0830-1130 100% ID CARD CHECKS AT MAIN GATE
1000-1300 100% ID CARD CHECKS AT BACK GATE
1305-1505 MWD PRESENCE AT MAIN GATE (MEASURE 30)
1305-1505 RANDOM VEHICLE INSPECTION AT MAIN GATE (MEASURE 1)
1615-1815 100% ID CARD CHECKS AT BACK GATE
1800-2100 100% ID CARD CHECKS AT MAIN GATE

MCBXYZ RAM totals:

CAT 1 RAMS (MWD EMPLOYMENT): 14 HOURS
CAT 2 RAMS (RANDOM VEHICLE INSPECTIONS): 15 HOURS
CAT 3 RAMS (PERSONNEL INSPECTIONS / ID CHECKS): 209 HOURS
CAT 4 RAMS (ADDITIONAL RAMS): 23 HOURS

January	Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1	2	3	4	5	6 4	7
	8	9	10	11	12	13 7	14
	15	16	17	18	19	20 3	21
	22	23	24	25	26	27 2	28
2007	29	30	31				

February	Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3 3	4
	5	6	7	8	9	10 6	11
	12	13	14	15	16	17 1	18
	19	20	21	22	23	24 4	25
2007	26	27	28				

March	Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3 5	4
	5	6	7	8	9	10 1	11
	12	13	14	15	16	17 6	18
	19	20	21	22	23	24 4	25
2007	26	27	28	29	30	31 3	

April	Mon	Tue	Wed	Thu	Fri	Sat	Sun
							1
	2	3	4	5	6	7 2	8
	9	10	11	12	13	14 4	15
	16	17	18	19	20	21 2	22
2007	23	24	25	26	27	28 5	29
	30						

APPENDIX H

SAMPLE SEPARATE AT PLAN



UNITED STATES MARINE CORPS

COMMANDER, U.S. MARINE CORPS FORCES, PACIFIC
CAMP H.M. SMITH, HI 96861-5001

IN REPLY REFER TO:

3000
G3, AT
03 Apr 08

From: Commander JTF Cobra Gold 08
To: Exercise Cobra Gold 08 Participants

Subj: ANTITERRORISM PLAN FOR EXERCISE COBRA GOLD 08 AND RELATED
HUMANITARIAN CIVIC ACTION ACTIVITIES

Ref: (a) USPACOM OPORD 5050-08, 18 Mar 08
(b) Defense Intelligence Agency World Wide Threat Levels
http://www.dia.smil.mil/intel/world_wide/threat/AppendixA.html
(c) MARFORPAC OPORD 06-01, 13 Nov 06
(d) DoD I 2000.16, 08 Dec 06
(e) COMMARFORPAC msg R 252224Z MAR 08, Blanket Theater and
Country Clearance Request For Thailand
(f) COMMARFORPAC msg R 011926Z APR 08, CG08 FORWARD/REAR
ACTIVATION MESSAGE
(g) JTF Cobra Gold 08 Handbook

Encl: (1) Force Protection Conditions (FPCONs)
(2) Blue Dart Reporting Procedures
(3) Blue Dart Telephonic Report Format
(4) Blue Dart Follow-Up Genser Message Format
(5) Emergency Phone Numbers
(6) JS Guide 526
(7) FP Smart Card (To Be Published Separately)

1. (U) **Situation.** Reference (a) requires submission of an Antiterrorism (AT) plan for Department of Defense (DoD) personnel traveling in foreign areas with a recognizable terrorist threat. The following information is provided in compliance with references (a) through (g) for the travel of Exercise Cobra Gold 08 personnel to the Kingdom of Thailand for participation in Exercise Cobra Gold and related Humanitarian

Civic Action Activities. U.S. Marine Corps Force Pacific (MARFORPAC) is the U.S. Executive Agent (EA) for Exercise Cobra Gold 08 (CG 08). CG 08 and related HCA activities will be conducted in multiple locations in Thailand, including Khorat, Utaphao, Sattahip, Sameasan, Hat Yao, Chuk Samet, Lop Buri, Petcha Buri, Thung Prong, Rayong, Ban Chan Krem, Hat Khlod, Surat Thani, and Pran Buri. U.S. lodging in Thailand will be arranged at approved hotels surveyed by MARFORPAC AT Office or the FP Detachment-Thailand and for which current vulnerability assessment reports are on hand.

- a. (U) Participating Countries. United States and Thailand as co-hosts.
- b. (U) Observing Countries. Indonesia, Japan, and Singapore.
- c. (U) Threat.

(1) (U) Threat Situation: There is no threat reporting that indicates any terrorist group or criminal element in Thailand is targeting Americans in general, or CG 08 participants in particular. Currently, there are both Department of State (DoS) travel notices and USPACOM Travel Restrictions in place for Thailand. USPACOM has a travel restriction for the four southernmost provinces of Songkhala, Pattani, Yala, and Narathiwat, as well as the city of Hat Yai, because they have been the scene of religious/ethnic violence for nearly 3 years. No CG 08 activities will take place in any travel-restricted areas. Absent such reporting, standard individual protective measures and safety precautions should suffice. The JS Guide 5260 is at enclosure (5) to this plan, and should be carried by all travelers. Deployment planners should consult the DoD Foreign Clearance Guide (www.fcg.pentagon.mil/fcg) before travel for the most current information regarding advisories and restrictions.

(2) (U) Threat Level: Current Defense Intelligence Agency (DIA) threat levels and other country information for countries within the PACOM Area of Responsibility (AOR) are available from the USPACOM J34 SIPRNET home page at:
http://www.hq.pacom.smil.mil/j3/j34/Status/country_reqts.doc.

(3) (U) Threat Assessment: At the time of this writing, Thailand's DIA-assessed Terrorist Threat Level is SIGNIFICANT. The DoS-assessed Criminal Threat Level is MODERATE. The Foreign Intelligence Service threat is assessed as MODERATE. The

current Force Health assessment for Thailand is MODERATE. For the most current threat assessment(s) or emergent data, travelers may contact the FPD; their telephone number is 011-662-287-1036 ext. 149.

(a) (U) Terrorism can be divided into two subcategories: domestic and international. Most of the press in recent months has been about domestic terrorism in the southern five provinces of Thailand. Currently, there have been no indications that U.S. personnel have been specifically targeted by these domestic terrorist incidents. By contrast, international terrorists, including al Qaeda and associated groups, have indicated their intent to attack Americans worldwide whenever and wherever possible. Although no indications currently exist of an al Qaeda or related group's intent to attack American personnel, this possibility can never be fully discounted and is underscored by the August 2003 capture of an alleged senior operative of Jemaah Islamiyah/al Qaeda in Ayuttaya, north of Bangkok. As standard FP guidance to all deployed U.S. military personnel, personnel are encouraged to practice standard personal protective measures and maintain a high degree of awareness of their surroundings. Unusual or suspicious incidents should be reported immediately to local FP officers or counterintelligence personnel.

(b) (U) Criminal activity represents a significant threat to U.S. service members during non-duty periods, considering that most will leave the hotel for shopping, dining, and sightseeing. Criminal activity aimed at U.S. service members will most likely include pick pocketing, petty theft, and scams. Scams include local tours at inflated prices, sales of counterfeit goods and jewelry, and price-gouging directed toward U.S. service members.

(c) (U) The threat from Foreign Intelligence Services is present in almost every country and Thailand is no different. One of the best things that individuals can do to keep information out of the enemy's hands is to practice good Operations Security (OPSEC). CG 08 will involve both unclassified and classified activities. In addition to OPSEC, never discuss classified information outside of a secure area, or inside a secure area where you are unsure of the clearance or access of the personnel present. Always report any attempt at elicitation immediately.

(d) (U) The Force Health includes safety issues and health issues. Thai drivers often drive with excessive speed and little regard for traffic laws. This represents a safety threat to U.S. service members who are attempting to cross the street during hours of heavy traffic because Thai drivers can often be unpredictable and do not follow what U.S. service members would expect as normal driving patterns. Moreover, those personnel not accustomed to countries where motorists drive on the left side, like Thailand, inadvertently place themselves at risk by looking the wrong way when crossing streets. Health-related concerns take on several different forms. Thailand is widely reputed to have endemic levels of sexually transmitted diseases, including HIV/AIDS and various strains of Hepatitis. Whereas some of the actual statistics and percentages are disputed among health professionals, and government public health programs have been successful at reducing the rate of growth in new cases, the general consensus is the numbers are much higher than other similarly sized countries. Contributing to this threat is the large sex industry in Thailand. Personnel considering engaging in sexual intercourse should be aware of this threat and protect themselves accordingly. Food and waterborne illnesses are also a significant threat. Tap water is not potable and should be avoided, even in hotels. Food should be cooked thoroughly and purchased only from reputable vendors. Swimming is off limits in the Sattahip area because of the presence of raw sewage.

(4) (U) Vulnerability Assessment: The JTF CG 08 Force Protection Coordination Cell (FPCC) assesses the vulnerability of CG 08 participating U.S. personnel, facilities, and equipment as negligible in most environments. CG 08 participants will arrive in Thailand individually or in small groups, in civilian clothing, on various airlines, on different times and dates. The presence of the FPD-Thailand ensures that CG 08 participants will benefit from the latest threat updates and their continuous coordination with host nation police authorities, regardless of location.

(5) (U) Risk Assessment:

(a) (U) The risk to U.S. participants in the CG 08 from the following threats is assessed as follows:

(1) (U) Terrorism: Low

(2) (U) Foreign Intelligence Services: Moderate

(3) (U) Criminal: Moderate

(4) (U) Force Health: Moderate

(b) (U) Based on this risk assessment, the following policies/procedures will be in place to mitigate these risks:

(1) (U) Terrorism: Existing FPCON with additional measures, including the Buddy Rule and individual AT training and awareness levels, coupled with close coordination with the FPD are sufficient to mitigate any terrorist threat currently anticipated against CG 08 activities.

(2) (U) Foreign Intelligence Services: CG 08 will involve both classified and unclassified activities. U.S. participants must not discuss classified information outside secured areas and should immediately report any attempts at elicitation by any foreign persons, regardless of location or topic.

(3) (U) Criminal: All CG 08 U.S. participants are required to use the Buddy System. Avoid suspicious persons and areas. Maintain your situational awareness at all times.

(4) (U) Force Health: U.S. Military vehicles, JUSMAG-arranged transport, hotel-operated shuttles, and meter taxis are acceptable forms of transportation, in descending order of preference. In the event of non-emergency medical issues that require treatment, contact JUSMAG-Thai during normal duty hours for TRICARE referral to the nearest suitable medical treatment facility. Drink only bottled water, and consume food from known, reputable sources. Travelers who are prone to bacterial illness should avoid antacids. Wash hands often with soap/water and/or antibacterial hand sanitizer.

(6) (U) Force Protection Condition (FPCC). The current FPCON for Thailand is ALPHA/BRAVO with additional measures. The additional measures directed by USPACOM and Commander Joint Task Force (explained in detail in Enclosure (1)) are:

(a) (U) USPACOM directed additional measures:

- FPCON BRAVO measures:

- Measure BRAVO 4. Secure and inspect all buildings, rooms, and storage areas not in regular use.
 - Measure BRAVO 5. At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.
 - Measure BRAVO 13. Conduct random patrols to check vehicles, people, and buildings.
- Shipboard BRAVO measures:
- Measure BRAVO 6. Post signs in local language specifying visiting and loitering restrictions clearly.
 - Measure BRAVO 7. When in a non-U.S. Government controlled port, identify and randomly inspect authorized watercraft, such as workboats, ferries and commercially rented liberty launches, daily.
 - Measure BRAVO 9. Inspect all visitors' hand-carried items, and packages before allowing them aboard. Where available, use baggage scanners and walk-through or handheld metal detectors to screen visitors and their packages before boarding the ship.
 - Measure BRAVO 10. Implement measures to keep unauthorized craft away from the ship. Authorized craft should be carefully controlled. Coordinate with host nation's husbanding agent/local port authority, as necessary, and request their assistance in controlling unauthorized craft.

(b) (U) Commander Joint Task Force directed additional measures:

- Deployed BRAVO measures:
- Deployed Unit Measure BRAVO 6. Brief command representatives of all units and activities at the deployment site concerning the threat and security measures implemented in response to the threat. Implement procedures to provide periodic updates for these unit and activity representatives.

- Deployed Unit Measure BRAVO 9. Establish concentric zones of security. Assign sectors of responsibility to units to defend during an attack.
 - Deployed Unit Measure BRAVO 11. Implement the Buddy Rule for all personnel departing the deployment location. Review unit liberty policy and revise it as necessary to enhance force protection.
- Traveler BRAVO measures:
- Traveler Measure BRAVO 3. Do not travel with easily identifiable military luggage (i.e., duffel bags, B-4 bags) or military tags or organizational identification.
 - Traveler Measure BRAVO 6. Routinely check your vehicle(s) for bombs.
 - Traveler Measure BRAVO 9. Determine and avoid high-risk areas and be cautious of mingling with crowds.

Any changes to FPCON measures after release of this plan will be briefed upon arrival in Thailand. Consult the USPACOM J34 Web site (Web address 1.C.2, above) immediately before travel to obtain the latest FPCON status.

d. (U) Friendly:

(1) (U) Own Forces Locations. All arriving CG 08 participants transiting through Bangkok/Korat will receive an FP Smart Card containing contact phone numbers, emergency phone numbers, FP travel tips, and select phrases in Thai enclosure (6). All arriving CG 08 participants will also receive an Exercise CG 08 FP brief before transiting to their exercise locations, HCA sites, or billeting locations. Those participating in the JTF Forward/Rear will RON at one of the approved contracted hotels in Bangkok for the entirety of their visit.

(2) (U) Host Nation Security Capability. Royal Thai Supreme Command (RTSC) in consultation with JUSMAGTHAI will provide information to local police. All Exercise CG 08 force bed-down sites will be conducted on Thai military installations or pre-selected HCA sites, with Thai and JUSMAG escort officers. Mr. David Turner, Force Protection Detachment, will be apprised of

non-scheduled movements - FPD contact information is at Enclosure (4).

2. (U) Mission. To provide AT awareness and FP of U.S. Forces during deployment; training and HCA activities; and redeployment for exercise CG 08 participants.

3. (U) Execution

a. (U) Commander's Intent. FP is the first priority of all Exercise CG 08 participants during all phases of this exercise. CG 08 participants will maintain awareness and comply with all FPCON measures described in this plan. The FPCON set during the timeframe of each event will drive the specific measures. For example, if the FPCON for Thailand is increased to BRAVO, all CG 08 participants will comply with the FPCON Normal through BRAVO measures described in Enclosure (1, as well as any additional measures provided by Commander JTF CG 08 FPCC. JTF FPCC representatives will maintain liaison with host nation, JUSMAGTHAI and the U.S. Embassy to ensure proper security measures are in place and timely threat information is passed.

b. (U) Concept of Operations.

(1) (U) Physical Security:

(a) (U) During the exercise, the Royal Thai Supreme Command HQ (RTSC HQ) is responsible for overall FP of Exercise CG 08 participants. All requests for specific Thai support, including military, police, and Thai civilian support, will be routed through the JTF CG 08 FPCC. The RTSC will affect all aspects of required Thai military and government coordination.

(b) (U) Physical Security at Exercise Site(s). Host nation is responsible for securing the outward borders of all exercise billeting, concentration and/or training areas. Participating forces are responsible for securing the billeting, concentration and/or training areas. The host nation and U.S. security forces must be able to maintain FPCON A with specified USPACOM additional measures, as well as those additional measures specified by the JTF at all times.

(c) (U) Physical security at Bed-Down Site(s). Units using commercial hotels for billeting will billet in only those hotels with vulnerability assessments approved by the JUSMAGTHAI FPD. Units using commercial hotels will designate an FP

representative, including an alternate, who is available 24 hours a day to receive, report, and disseminate threat information and instructions to all personnel residing at these sites. Reporting requirements will be conducted through secure communication, if available, and cell phone as an alternate means of communication. The JTF CG 08 FPCC will coordinate any requests for additional host nation police at billeting points that require security beyond what is provided by hotel security.

(2) (U) Transportation Security. FPD-Thailand will be made aware of the movement itineraries to all exercise force bed-down sites, HCA sites, and routes of travel. Vehicle movement will be conducted in convoy when feasible. Each vehicle should have one occupant with a cell phone.

(3) (U) Arming of Security Personnel/Participants. In accordance with (IAW) U.S. and host nation agreements, no U.S. personnel will be armed in support of Exercise CG 08.

(4) (U) FPCON Measures. The key to security at this event will be individual awareness. All measures for the FPCON in effect during travel will be complied with, plus additional measures directed by USPACOM, MARFORPAC, or other competent authority. All FPCON measures are listed in Enclosure (1).

(5) (U) Emergency Action Plan.

(a) (U) In the event of emergency conditions, all participating units/personnel must be prepared to execute the following additional measures upon direction:

- FPCON BRAVO measures:

- Measure BRAVO 2. Enforce control of entry onto U.S. infrastructure critical to mission accomplishment, lucrative targets, and high-profile locations; and randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large improvised explosive device (IED) (cargo vans, delivery vehicles) sufficient to cause catastrophic damage or loss of life.
- Measure BRAVO 17. As deemed appropriate, verify identity of personnel entering buildings.

- FPCON CHARLIE measures:
 - Measure CHARLIE 4. Limit access points to strictly enforce entry. Randomly search vehicles.
 - Measure CHARLIE 9. Protect all designated infrastructure critical to mission accomplishment. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.
 - Measure CHARLIE 10. To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

- Deployed BRAVO measure:
 - Deployed Unit Measure BRAVO 10. Ensure personnel traveling away from the deployment site leave at least one individual to protect and secure vehicles in unsecured areas. Implement a convoy security plan for all vehicles leaving the deployment site.

- Deployed CHARLIE measures:
 - Deployed Unit Measure CHARLIE 3. Implement a two-vehicle rule for all vehicles exiting secured areas.
 - Deployed Unit Measure CHARLIE 7. Request host nation law enforcement to provide additional security for vehicles traveling away from the deployment site.
 - Deployed Unit Measure CHARLIE 9. Implement centralized parking for all vehicles. Park vehicles at least 100 meters away from sensitive areas. Implement a shuttle service if required.
 - Deployed Unit Measure CHARLIE 12. Cancel unit liberty. Execute emergency recall.
 - Deployed Unit Measure CHARLIE 13. Cancel all official social events. Advise all personnel to severely limit social

activities. Place all high-risk areas off limits.

(b) (U) In the event of an emergency while at a HCA site or any other field location, CG 08 participants will remain in place and take necessary measures for security and protection. Communicate the situation to organic and host nation authorities for security, fire, and medical response. CG 08 participants will mitigate any threat by maintaining accountability of personnel and rendering medical aid to the wounded and injured. If the situation dictates, participants will move to the closest Thai Military Base, report their change of location to the FPCC, and await further guidance.

(c) (U) In the event of an emergency while at the hotel, exercise participants will follow the instructions of hotel staff and/or emergency responders, and the U.S. Embassy will be contacted for guidance. In the event of a hotel evacuation, predesignated muster points will be used.

4. (U) Administration and Logistics

a. (U) Administration.

(1) (U) The JTF Forward/Rear G1 in conjunction with each component representatives will maintain daily accountability of U.S. military personnel by location. Per reference (f), all personnel who will arrive at Bangkok before 12 Apr 2008, must contact the JTF FWD/REAR SNCOIC GySgt Parris, at the CG 08 FWD/REAR Administration Office at ext. 708. Daily report times via cell phone will be at 0630 and 1830 daily. A roster of all exercise personnel in Thailand will be provided to FPD-Thailand as required.

(2) (U) All commands participating in CG 08 must direct their exercise participants to process through the Joint Reception Center (JRC) for accountability purposes upon their arrival at Bangkok. In particular, commands must ensure reservists deploying to Bangkok are fully briefed on the CG 08 JRC processing requirements, and that the reservists are given their ULNS before deployment to Thailand. Onward assistance to exercise final destination will be provided by the JRC. As a reminder, all personnel arriving via commercial carrier through BKK are required to have a valid passport in their possession.

Visas are required for those personnel arriving via commercial carrier and staying more than 30 days.

(3) (U) Further, component reps will report by exception any incidents, accidents, or suspicious incidents involving their personnel to the JTF CG 08 FPCC Forward/Rear in Bangkok, Thai cell # 08 7993 3234 and/or JTF HQ, FPCC Khorat, Thai cell # 08 5247 5461.

b. (U) Logistics.

(1) (U) Transportation:

(a) (U) Ground transportation to and from the airport will be made by the JTF Forward/Rear G4. Ground transportation between hotels and force bed-down locations will be coordinated between JTF G4 and Contracting Officers, and JUSMAG-Thai.

(b) (U) Per reference (f), all commands and personnel are strongly encouraged to call or e-mail appropriate JTF (FWD/REAR) personnel regarding any questions pertaining to TMO (shipping and customs), personnel arrivals, or any other issues at any time to ensure proper coordination and situational awareness.

(2) (U) Medical and Health:

(a) (U) Routine medical assistance will be conducted by unit medical personnel or coordinated with the Medical Nurse at JUSMAGTHAI.

(b) (U) There are several U.S. Embassy approved hospitals for visiting forces within Thailand; their names and contact information are at enclosure (4). These hospitals provide emergency trauma services and are TRICARE approved.

(3) (U) In accordance with reference A, USPACOM guidance regarding leave in conjunction with official travel will be adhered to by all participants. Leave travel requires completion of a separate FP plan to cover the leave travel portion.

5. (U) Command and Signal

a. (U) Signal: Primary means of reporting daily personnel accountability or passing information will be via landline phone, SAT phone, SIPRNET/NIPRNET, cell phone, or personal contact. Threat information will be immediately disseminated to the affected personnel, then through the FPD via the most expeditious means possible. Secondary means of passing information will be cell phones. The JTF CG 08 FPCC Chief and other staff members will have cell phones. It is strongly recommended that all participants conducting independent travel to and from Thailand, have cell phones and that their contact information be listed on their individual FP/emergency plans held at their respective commands. Enclosure (4) lists emergency contact numbers for Thailand.

b. (U) Notification: The JTF CG 08 FPCC representative will maintain contact with the MARFORPAC Force Command Center (DSN: 315-477-0077; Toll Free: 1-800-445-1708, Commercial: 001-808-477-0077) and JUSMAGTHAI at the beginning and end of the deployment, and as circumstances warrant in between.

c. (U) Command. The Commander JTF CG 08 will exercise control of FPCON measures through the JTF CG 08 FPCC Chief, Mr. Ted Hashimoto or Paul Allen MARFORPAC ATO. All Exercise CG 08 participants will comply with the measures listed in this plan, as well as any additional measures subsequently passed during any of the phases of Exercise CG 08. FPD-Thailand has overall responsibility for counterintelligence operations during this event.

By Direction

ENCLOSURE (1): FPCON Measures

1. General.

a. FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

b. FPCON ALPHA applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

c. FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and impact relations with local authorities.

d. FPCON CHARLIE applies when an incident occurs or intelligence is received indicating that some form of terrorist action or targeting against personnel or facilities is likely. Implementation of CHARLIE measures will create hardship and affect the activities of the unit and its personnel.

e. FPCON 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 imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

2. Basic FPCON Measures.

a. FPCON NORMAL Measures

(1) Measure NORMAL 1. Secure and randomly inspect buildings, rooms, and storage areas not in regular use.

(2) Measure NORMAL 2. Conduct random security spot-checks of vehicles and persons entering facilities under the jurisdiction of the United States.

(3) Measure NORMAL 3. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

(4) Measure NORMAL 4. Conduct mitigation, preparedness, response and recovery planning activities to deter, detect and defend against CBRNE attacks.

b. FPCON ALPHA Measures

(1) Measure ALPHA 1. Continue, or introduce, all measures in previous FPCON.

(2) Measure ALPHA 2. At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.

(3) Measure ALPHA 3. The duty officer or personnel with access to building plans, as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available.

(4) Measure ALPHA 4. Increase security spot-checks of vehicles and persons entering installations under the jurisdiction of the United States.

(5) Measure ALPHA 5. Initiate food and water Operational Risk Management (ORM) procedures, brief personnel on food and water security procedures, and report any unusual activities.

(6) Measure ALPHA 6. Test mass notification system.

(7) Measure ALPHA 7. Review all plans, identify resource requirements, and be prepared to implement higher FPCONs.

(8) Measure ALPHA 8. Review and, if necessary, implement security measures for high-risk personnel.

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

(10) Measure ALPHA 10. Review intelligence, counter-intelligence, and operations dissemination procedures.

c. FPCON BRAVO Measures

(1) Measure BRAVO 1. Continue, or introduce, all measures in previous FPCONS.

(2) Measure BRAVO 2. Enforce control of entry onto U.S. infrastructure critical to mission accomplishment, lucrative targets, and high-profile locations; and randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles capable of concealing a large IED (cargo vans, delivery vehicles) sufficient to cause catastrophic damage or loss of life.

(3) Measure BRAVO 3. Identify critical and high-occupancy buildings. Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality; the protection level provided by structure, IED/Vehicle Borne IED threat; and available security measures. Consider centralized parking.

(4) Measure BRAVO 4. Secure and inspect all buildings, rooms, and storage areas not in regular use.

(5) Measure BRAVO 5. At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

(6) Measure BRAVO 6. Implement mail-screening procedures to identify suspicious letters and parcels.

(7) Measure BRAVO 7. Randomly inspect commercial deliveries. Advise family members to check home deliveries.

(8) Measure BRAVO 8. Randomly inspect food and water for evidence of tampering/contamination before use by Department of Defense (DoD) personnel. Inspections should include delivery vehicles and storage area/containers.

(9) Measure BRAVO 9. Increase security/guard presence or patrol/surveillance of DoD housing areas, schools, messes, on-base clubs, and similar high-occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

(10) Measure BRAVO 10. Implement plans to enhance off-installation security of DoD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and family members.

(11) Measure BRAVO 11. Inform local security committees of actions being taken.

(12) Measure BRAVO 12. Verify identity of visitors and randomly inspect their suitcases, parcels, and other containers.

(13) Measure BRAVO 13. Conduct random patrols to check vehicles, people, and buildings.

(14) Measure BRAVO 14. As necessary, implement additional security measures for high-risk personnel.

(15) Measure BRAVO 15. Place personnel required for implementing AT plans on call; commanders should exercise discretion in approving absences.

(16) Measure BRAVO 16. Identify and brief personnel who may augment guard forces. Review specific rules of engagement, including the use of deadly force.

(17) Measure BRAVO 17. As deemed appropriate, verify identity of personnel entering buildings.

(18) Measure BRAVO 18. Review status and adjust as appropriate OPSEC, COMSEC, and INFOSEC procedures.

(19) Measure BRAVO 19. (Airfield-specific) As appropriate, erect barriers and staff and establish checkpoints at entrances to airfields. Ensure identity of all individuals entering the airfield (flightline and support facilities) - no exceptions. Randomly inspect vehicles, briefcases, and packages entering the airfield.

(20) Measure BRAVO 20. (Airfield-specific) Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate threat of surface-to-air missiles or

standoff weapons that can be delivered from beyond the airfield perimeter.

d. FPCON CHARLIE Measures

(1) Measure CHARLIE 1. Continue, or introduce, all measures in previous FPCON.

(2) Measure CHARLIE 2. Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and Status of Forces Agreements (SOFAs). Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapons capabilities.

(3) Measure CHARLIE 3. Be prepared to react to requests for assistance, from both local authorities and other installations in the region.

(4) Measure CHARLIE 4. Limit access points to strictly enforce entry. Randomly search vehicles.

(5) Measure CHARLIE 5. Ensure or verify identity of all individuals entering food and water storage and distribution centers, use sign in/out logs at access control/entry points, and limit and/or inspect all personal items.

(6) Measure CHARLIE 6. Initiate contingency monitoring for biological and chemical agents as required. Suspend contractors/off-facility users from tapping into facility water system (alternate locally developed measure should be executed when contractors are responsible for DoD water supplies or when water is provided by local (non-DoD) sources or agencies).

(7) Measure CHARLIE 7. Increase standoff from sensitive buildings based on threat. Implement barrier plan to hinder vehicle-borne attack.

(8) Measure CHARLIE 8. Increase patrolling of the facility to include waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions/persons outside the facility perimeter. For airfields, patrol or provide observation of approach and departure flight corridors as appropriate to the threat (coordinate with the Transportation Security Administration (TSA), Marine Patrol,

U.S. Coast Guard (USCG), and local law enforcement as required to cover off-facility approach and departure flight corridors).

(9) Measure CHARLIE 9. Protect all designated infrastructure critical to mission accomplishment. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

(10) Measure CHARLIE 10. To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

(11) Measure CHARLIE 11. Consider searching suitcases, briefcases, packages, etc., being brought onto the installation through access control points and consider randomly searching suitcases, briefcases, packages, etc., leaving.

(12) Measure CHARLIE 12. Review personnel policy procedures to determine course of action for family members.

(13) Measure CHARLIE 13. Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flightline and support facilities.

(14) Measure CHARLIE 14. Consider escorting children to and from DoD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.).

(15) Measure CHARLIE 15. (Airfield-specific) Reduce flying to essential operational flights only. Implement appropriate flying countermeasures as directed by the Flight Wing Commander (military aircraft) or TSA (civilian aircraft). Consider relief landing ground actions to take for aircraft diversions into and out of an attacked airfield. Consider augmenting firefighting details.

e. FPCON DELTA Measures

(1) Measure DELTA 1. Continue or introduce all measures in previous FPCON.

(2) Measure DELTA 2. Augment guards as necessary.

(3) Measure DELTA 3. Identify all vehicles within operational or mission support areas.

(4) Measure DELTA 4. Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles used to transport escorted VIPs are exempted.

(5) Measure DELTA 5. Control facility access and implement positive identification of all personnel - no exceptions.

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

(7) Measure DELTA 7. Close DoD schools and/or escort children to/from DoD schools as required.

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

(9) Measure DELTA 9. Restrict all non-essential movement.

(10) Measure DELTA 10. (Airfield-specific) Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft and/or helicopters for surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

(11) Measure DELTA 11. (Airfield-specific) As appropriate, airfields should prepare to accept aircraft diverted from other stations.

(12) Measure DELTA 12. If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

3. Shipboard FPCON Measures.

a. FPCON NORMAL Measures

(1) Measure NORMAL 1. Brief crew on the port-specific threat, the security/AT plan, and security precautions to be taken while ashore. Ensure all hands are knowledgeable of various FPCON requirements and that they understand their roles in implementation of measures.

(2) Measure NORMAL 2. Remind all personnel to be suspicious and inquisitive of strangers, be alert for abandoned parcels or suitcases and for unattended vehicles in the vicinity. Report unusual activities to the OOD, Master or Mate on watch, as applicable.

(3) Measure NORMAL 3. Secure and periodically inspect spaces not in use.

(4) Measure NORMAL 4. Review security plans and keep them available.

(5) Measure NORMAL 5. Review pier and shipboard access control procedures, including land and water barriers.

(6) Measure NORMAL 6. Ensure sentries/Mate on Watch, roving patrols and the quarterdeck/gangway watch have the ability to communicate with each other.

(7) Measure NORMAL 7. Coordinate pier/fleet landing security requirements with SOFA, collocated forces, and/or husbanding agent. Identify anticipated needs for mutual support and define methods of implementation and communication.

b. FPCON ALPHA Measures

(1) Measure ALPHA 1. Muster, arm, and brief security personnel on the threat and rules of engagement. Keep key personnel who may be needed to implement security measures on call.

(2) Measure ALPHA 2. U.S.Navy (USN) combatant ships when in a non-USN controlled port, deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside the United States (minimum standoff distances). DoD non-combatants in a non-U.S. Government controlled port, request husband agent arrange and deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside the United States (minimum standoff distances).

(3) Measure ALPHA 3. (USN combatant ship-specific) Randomly inspect vehicles entering pier.

(4) Measure ALPHA 4. Randomly inspect hand-carried items and packages before they are brought aboard.

(5) Measure ALPHA 5. Regulate shipboard lighting to best meet the threat environment.

(6) Measure ALPHA 6. When in a non-U.S. Government controlled port, rig hawsepipes covers and rat guards on lines, cables, and hoses. Consider using an anchor collar.

(7) Measure ALPHA 7. When in a non-U.S. Government controlled port, raise accommodation ladders, stern gates, ladders, etc., when not in use.

(8) Measure ALPHA 8. Increase frequency of security drills.

(9) Measure ALPHA 9. Establish internal and external communications, including connectivity checks with local operational commander/agencies/authorities that will be expected to provide support, if required.

c. FPCON BRAVO Measures

(1) Measure BRAVO 1. Continue or introduce all measures in previous FPCON.

(2) Measure BRAVO 2. Set Material Condition YOKE--Secure all watertight door and hatches, main deck, and below.

(3) Measure BRAVO 3. Consistent with local rules, regulations, and/or the SOFA: USN combatant ships post armed pier sentries as necessary; and non-combatant ships post pier sentries (armed at the Master's discretion) as necessary.

(4) Measure BRAVO 4. Restrict vehicle access to the pier. Discontinue parking on the pier. Consistent with local rules, regulations, and/or the SOFA, establish unloading zones and move all containers as far away from the ship as possible (recommend 100 feet in the United States, 400 feet outside the United States as the minimum stand-off distance).

(5) Measure BRAVO 5. Consistent with the local rules, regulations, and/or the SOFA: USN combatant ships post additional armed watches as necessary; and non-combatant ships post additional watches (armed at the Master's discretion) as necessary. Local threat, environment, and fields of fire should be considered when selecting weapons.

(6) Measure BRAVO 6. Post signs in local language specifying visiting and loitering restrictions clearly.

(7) Measure BRAVO 7. When in a non-U.S. Government controlled port, identify and randomly inspect authorized watercraft, such as workboats, ferries, and commercially rented liberty launches, daily.

(8) Measure BRAVO 8. When in a non-U.S. Government controlled port, direct liberty boats to make a security tour around the ship upon departing from and arriving at the ship, with particular focus on the waterline and under pilings when berthed at a pier.

(9) Measure BRAVO 9. Inspect all visitors' hand-carried items and packages before allowing them aboard. Where available, use baggage scanners and walk-through or handheld metal detectors to screen visitors and their packages before boarding the ship.

(10) Measure BRAVO 10. Implement measures to keep unauthorized craft away from the ship. Authorized craft should be carefully controlled. Coordinate with host nation's husbanding agent/local port authority, as necessary, and request their assistance in controlling unauthorized craft.

(11) Measure BRAVO 11. Raise accommodation ladders, etc, when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

(12) Measure BRAVO 12. Review liberty policy in light of the threat and revise it, as necessary to maintain safety and security of ship and crew.

(13) Measure BRAVO 13. USN combatant ships conduct division quarters at foul weather parade. All DoD ships avoid conducting activities that will gather large number of crewmembers at the weatherdecks. Where possible, relocate such activities inside the skin of the ship.

(14) Measure BRAVO 14. Ensure an up-to-date list of bilingual personnel for area of operations is readily available. Maintain warning tape, in both the local language and English, is in bridge/pilot house/quarterdeck, for use on the ship's announcing system to warn small craft to remain clear.

(15) Measure BRAVO 15. If not already armed, arm the quarterdeck/gangway or mate on watch.

(16) Measure BRAVO 16. If not already armed, consider arming the sounding and security patrol.

(17) Measure BRAVO 17. Review procedures for expedient issue of firearms and ammunition to the shipboard self-defense force (SSDF)/reaction force and other members of the crew, as deemed necessary by the commanding officer/master.

(18) Measure BRAVO 18. Instruct watches to conduct frequent, random searches of pier, including pilings and access points.

(19) Measure BRAVO 19. Conduct visual inspections of the ship's hull and ship's boats at intermittent intervals and immediately before it is put to sea using both landside personnel and waterside patrols.

(20) Measure BRAVO 20. Hoist ships boats aboard when not in use.

(21) Measure BRAVO 21. Terminate all public visits. In U.S. Government controlled ports, host visits (family, friends, small groups sponsored by the ship) may continue at the Commanding Officer's/Master's discretion.

(22) Measure BRAVO 22. After working hours, reduce entry points to ship's interior by securing infrequently used entrances. Safety requirements must be considered.

(23) Measure BRAVO 23. In non-U.S. Government controlled ports, use only one brow/gangway to access ship (remove any excess brows/gangways). CV(N)s and other large decks may use two as required, when included in an approved AT Plan specific to that port visit.

(24) Measure BRAVO 24. In non-U.S. Government controlled ports, maintain capability to get under way on short notice or as specified by standard operating procedures.

(25) Measure BRAVO 25. In non-U.S. Government controlled ports, consider layout of fire hoses. Brief designated crew personnel on procedures for repelling boards, small boats and ultra-light aircraft.

(26) Measure BRAVO 26. Where applicable obstruct possible helicopter landing areas.

(27) Measure BRAVO 27. Where possible, monitor local communications (ship-to-ship, television, radio, police scanners, etc).

(28) Measure BRAVO 28. As appropriate, inform local authorities of actions being taken as FPCON increases.

(29) Measure BRAVO 29. (USN combatant ship specific) If the threat situation warrants, deploy picket boats to conduct patrols in the immediate vicinity of the ship. Brief boat crews and arm with appropriate weapons considering threat, the local environment, and fields of fire.

d. FPCON CHARLIE Measures

(1) Measure CHARLIE 1. Continue or introduce all measures in previous FPCON.

(2) Measure CHARLIE 2. Consider setting Material Condition Zebra (secure all access doors and hatches), main deck, and below.

(3) Measure CHARLIE 3. Cancel liberty. Execute emergency recall.

(4) Measure CHARLIE 4. Prepare to get underway on short notice. If conditions warrant, request permission to sortie/get underway.

(5) Measure CHARLIE 5. Block unnecessary vehicle access to the pier.

(6) Measure CHARLIE 6. Coordinate with host nation husbanding agent and/or local port authorities to establish small boat exclusion zone around ship.

(7) Measure CHARLIE 7. (USN combatant ship specific) Deploy the SSDF to protect command structure and augment posted watches. Station the SSDF in positions that provide 360 degrees coverage of the ship.

(8) Measure CHARLIE 8. Energize radar and or sonar, rotate screws and cycle ruder(s) at frequent and irregular intervals, as needed, to assist in deterring, detecting or thwarting attacks.

(9) Measure CHARLIE 9. Consider staffing repair locker(s). Be prepared to staff one repair locker on short notice. Ensure adequate lines of communications are established with damage control central.

(10) Measure CHARLIE 10. (USN combatant ship specific) If available and feasible, consider use of airborne assets as an observation/FP platform.

(11) Measure CHARLIE 11. If a threat of swimmer attack exists, activate an anti-swimmer watch.

(12) Measure CHARLIE 12. In non-U.S. Government controlled ports and if unable to get underway, consider requesting armed security augmentation from area Combatant Commander.

e. FPCON DELTA Measures

(1) Measure DELTA 1. Continue or introduce all measures in previous FPCON.

(2) Measure DELTA 2. Permit only necessary personnel topside.

(3) Measure DELTA 3. If possible, cancel port visit and get underway.

(4) Measure DELTA 4. Employ all necessary weaponry to defend against attack.

4. Deployed Unit FPCON Measures.

a. Deployed Unit FPCON NORMAL Measures

(1) Deployed Unit Measure NORMAL 1. Brief all deployed personnel on the current threat condition.

(2) Deployed Unit Measure NORMAL 2. Test radio and telephone communications monthly.

(3) Deployed Unit Measure NORMAL 3. Periodically exercise AT contingency plans and drills.

b. Deployed Unit FPCON ALPHA Measures

(1) Deployed Unit Measure ALPHA 1. Brief personnel for reason of higher FPCON. Review those AT measures enacted to increase security.

(2) Deployed Unit Measure ALPHA 2. Review unit-level terrorism awareness training.

(3) Deployed Unit Measure ALPHA 3. Increase liaison with local agencies via established chains of command to assist in monitoring potential threats. Notify local law enforcement if security measures could impact on their operations.

(4) Deployed Unit Measure ALPHA 4. As a deterrent, randomly use trained explosive ordnance detection dog (EODD) teams, if available.

(5) Deployed Unit Measure ALPHA 5. Advise all personnel of and to avoid high-risk areas and be cautious when mingling with crowds.

c. Deployed Unit FPCON BRAVO Measures

(1) Deployed Unit Measure BRAVO 1. Units will not deploy/travel into an area at FPCON BRAVO (or where this measure is directed) unless the first O-6 in the chain of command (or member of the senior executive service (SES) exercising equivalent authority) deems such travel to be mission essential and approves the AT plan for deployed units.

(2) Deployed Unit Measure BRAVO 2. Establish an operations watch/center to handle FP, including handling security posts, reaction forces, and responses to attack.

(3) Deployed Unit Measure BRAVO 3. Ensure all guard posts are staffed by at least two personnel and are armed with individual weapon and basic load.

(4) Deployed Unit Measure BRAVO 4. Provide for an armed reaction force.

(5) Deployed Unit Measure BRAVO 5. Notify local law enforcement concerning FPCON CHARLIE and DELTA security measures that could impact on their operations.

(6) Deployed Unit Measure BRAVO 6. Brief command representatives of all units and activities at the deployment site concerning the threat and security measures implemented in response to the threat. Implement procedures to provide periodic updates for these unit and activity representatives.

(7) Deployed Unit Measure BRAVO 7. Test radio and telephone communications weekly.

(8) Deployed Unit Measure BRAVO 8. Establish concentric zones of security. Assign sectors of responsibility to units to defend during an attack.

(9) Deployed Unit Measure BRAVO 9. Ensure personnel traveling away from the deployment site leave at least one individual to protect and secure vehicles in unsecured areas. Implement a convoy security plan for all vehicles leaving the deployment site.

(10) Deployed Unit Measure BRAVO 10. Implement the Buddy Rule for all personnel departing the deployment location. Review unit liberty policy and revise it as necessary to enhance FP.

d. Deployed Unit FPCON CHARLIE Measures

(1) Deployed Unit Measure CHARLIE 1. Units will not deploy/travel into an area at FPCON CHARLIE (or where this measure is directed) unless the first O-6 in the deploying unit's chain of command (or member of the senior executive service [SES] exercising equivalent authority) deems such travel to be mission essential. If an area is placed at FPCON CHARLIE or this measure is directed while deployed, contact your command to determine whether they are considering withdrawing the deployed force.

(2) Deployed Unit Measure CHARLIE 2. Units deploying to an area at FPCON CHARLIE will deploy with military police or other elements trained in terrorism counteraction.

(3) Deployed Unit Measure CHARLIE 3. Implement a two-vehicle rule for all vehicles exiting secured areas.

(4) Deployed Unit Measure CHARLIE 4. Put reaction force on 15-minute standby.

(5) Deployed Unit Measure CHARLIE 5. Provide ammunition for all armed personnel. Load weapons at the commander's discretion.

(6) Deployed Unit Measure CHARLIE 6. Request host nation law enforcement/security forces to augment/reinforce security forces.

(7) Deployed Unit Measure CHARLIE 7. Request host nation law enforcement to provide additional security for vehicles traveling away from the deployment site.

(8) Deployed Unit Measure CHARLIE 8. Conduct identity checks of all personnel entering the deployment site. Conduct detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) of all vehicles and interior inspections of all containers and packages.

(9) Deployed Unit Measure CHARLIE 9. Implement centralized parking for all vehicles. Park vehicles at least 100 meters away from sensitive areas. Implement a shuttle service if required.

(10) Deployed Unit Measure CHARLIE 10. If available, employ AT security devices, including ground surveillance radar, bomb detection devices, thermal imaging systems, etc.

(11) Deployed Unit Measure CHARLIE 11. Based on the threat, construct blast/defensive bunkers/positions to protect personnel in threatened areas.

(12) Deployed Unit Measure CHARLIE 12. Cancel unit liberty. Execute emergency recall.

(13) Deployed Unit Measure CHARLIE 13. Cancel all official social events. Advise all personnel to severely limit social activities. Place all high-risk areas off limits.

e. Deployed Unit FPCON DELTA Measures

(1) Deployed Unit Measure DELTA 1. Move personnel to blast/defensive bunkers.

(2) Deployed Unit Measure DELTA 2. As feasible, arm all available personnel.

(3) Deployed Unit Measure DELTA 3. Augment guard forces to ensure positive control and fires over the entire deployment site.

(4) Deployed Unit Measure DELTA 4. Frequently inspect outlying areas or exteriors of facilities and parking areas.

5. Traveler Measures.

a. Traveler FPCON NORMAL Measures

(1) Traveler Measure NORMAL 1. Obtain and follow measures the local commander or COM implements to increase security. Review AT awareness procedures.

(2) Traveler Measure NORMAL 2. Review your emergency action plan. Ensure all persons in party are familiar with the plan.

(3) Traveler Measure NORMAL 3. Confirm/identify protected and/or safe areas you can rapidly move to before/during an incident.

b. Traveler FPCON ALPHA Measures

(1) Traveler Measure ALPHA 1. For travel to countries below FPCON Bravo, the first O-5 in the chain of command is responsible for AT plan approval.

(2) Traveler Measure ALPHA 2. Maintain regular contact with the embassy RSO or nearest U.S. security agency/element, and/or local host nation security elements, as well as the home station.

(3) Traveler Measure ALPHA 3. Increase liaison with any available security agency (hotel, residential, etc.). Notify security agencies if security measures could impact their operations.

c. Traveler FPCON BRAVO Measures

(1) Traveler Measure BRAVO 1. For travel to countries at FPCON Bravo or higher, the first O-6 in the chain of command is responsible for AT plan approval. When applicable, a civilian

senior executive service (SES) or equivalent exercising authority satisfies these requirements.

(2) Traveler Measure BRAVO 2. Cease wearing U.S. military uniforms in non-secure areas.

(3) Traveler Measure BRAVO 3. Do not travel with easily identifiable military luggage (i.e., duffel bags, B-4 bags) or military tags or organizational identification.

(4) Traveler Measure BRAVO 4. Implement the Buddy Rule for all travelers, including leave and TDY/TAD missions.

(5) Traveler Measure BRAVO 5. Periodically exercise AT contingency plans and drills.

(6) Traveler Measure BRAVO 6. Routinely check your vehicle(s) for bombs.

(7) Traveler Measure BRAVO 7. Park your vehicle(s) in secure areas, not accessible to uncontrolled personnel.

(8) Traveler Measure BRAVO 8. Conduct weekly telephone liaison with embassy regional security officer or nearest U.S. security agency/element, and/or local host nation security elements and home station.

(9) Traveler Measure BRAVO 9. Determine and avoid high-risk areas and be cautious of mingling with crowds.

d. Traveler FPCON CHARLIE Measures

(1) Traveler Measure CHARLIE 1. If an area is placed at FPCON CHARLIE or this measure is directed during travel, contact your command to determine if they are considering withdrawing you or your party.

(2) Traveler Measure CHARLIE 2. Determine the nature of the imminent threat.

(3) Traveler Measure CHARLIE 3. Security personnel, trained in terrorism counteraction, will accompany large- or high-risk groups traveling to an area at FPCON CHARLIE.

(4) Traveler Measure CHARLIE 4. Coordinate with host nation law enforcement/ military to provide security when traveling

away from secured areas. Request host nation law enforcement and/or security forces provide and/or reinforce your protection detail.

(5) Traveler Measure CHARLIE 5. Conduct daily telephone liaison with embassy regional security officer or nearest U.S. security agency/element, and/or local host nation security elements and home station.

(6) Traveler Measure CHARLIE 6. Treat all mail packages as potential bombs. Conduct limited inspections for explosive or incendiary devices, or other dangerous items.

(7) Traveler Measure CHARLIE 7. Cancel all official social events. Severely limit social activities. Do not visit high-risk areas.

(8) Traveler Measure CHARLIE 8. Contact parent organization for guidance regarding continuation of leave, liberty, or passes.

(9) Traveler Measure CHARLIE 9. Cease wearing U.S. military uniforms.

e. Traveler FPCON DELTA Measures

(1) Traveler Measure DELTA 1. Move to a protected area.

(2) Traveler Measure DELTA 2. Treat all unidentified vehicles and containers as potential bombs.

(3) Traveler Measure DELTA 3. Minimize, cancel, or delay all non-essential movement.

(4) Traveler Measure DELTA 4. Conduct hourly telephone liaison with embassy regional security officer or nearest U.S. security agency/element, and/or local host nation security elements and home station.

(5) Traveler Measure DELTA 5. Cancel all social activities.

ENCLOSURE (2): USPACOM Blue Dart Reporting Procedures

1. USPACOM Blue Dart Reporting Procedure:

a. Within 30 minutes, contact the targeted element duty officer telephonically using a secure telephone, if possible. If not available, notify via unsecure telephone.

b. If the sending unit is unable to telephonically contact the targeted unit, BLUE DART information will be immediately telephoned to the USPACOM Command Duty Officer (CDO).

c. The CDO will then be responsible for disseminating telephonic BLUE DART threat information to the targeted command. Contact numbers for these duty officers are:

USPACOM: DSN XXX-XXX-XXXX or Comm. (XXX)XXX-XXXX
MFP COC: DSN XXX-XXX-XXXX or Comm. (XXX)XXX-XXXX
JTF CG 08 COC: XX-XXXX-XXXX within Thailand; dial XX-XX-XXXX-XXXX outside Thailand.

d. For BLUE DART information targeting a country without a military commander, contact the USPACOM CDO. CDO will disseminate information to the USPACOMREP or DATT in the targeted country.

e. The sender will provide all the information in the BLUE DART TELEPHONIC REPORTING FORMAT (Enclosure 3).

f. Receiving unit will conduct a call back to the sender of the BLUE DART, to authenticate the identity of the sender. Receiving unit will also maintain a written record of the BLUE DART information for future reference.

g. After dissemination of the threat to the targeted unit, the originator will transmit an immediate precedence follow-up GENSER message or DMS message over SIPRNET (with appropriate classification) within 2 hours of threat receipt. GENSER or DMS message will, at a minimum, be disseminated to the threatened command, USPACOMCDO, and organizations in AIG 988. The message will be in the BLUE DART FOLLOW-UP GENSER MESSAGE format (Enclosure 4).

ENCLOSURE (3): BLUE DART TELEPHONIC REPORTING FORMAT

a. Mandatory Lines:

1. "This is a real-world BLUE DART terrorist threat warning."

2. "This is (Caller's identity) from (Organization) and my unit telephone number is (Telephone number)."

3. "We have information there may be a terrorist attack on (Location/Person)."

b. Additional information to pass, if known:

1. "(Identity of attacker) will conduct the attack."

2. "The attacker will use (type of weapon) and the (method of attack)."

3. "The attack is being conducted because (reason for attack)."

c. "The source of the information is (general description of source's position, access, and reliability)." (NOTE: Only identify source if secure communications are available)

ENCLOSURE (4): BLUE DART FOLLOW-UP GENSER MESSAGE FORMAT

FM (Sending unit)
TO (Targeted unit)
INFO AIG 988
(Other commands deemed appropriate)

Classification: _____ -
SUBJ/BLUE DART

1. Threat: Specific information concerning terrorist attack which will include the following:

- a. Specific unit location or person to be attacked (mandatory).
- b. Specific time and date of attack (mandatory).
- c. Identity of attackers (if known).

- d. Identity type of weapon (bomb, rifle, etc.) to be used and the method of attack (if known).
 - e. Provide the reason for the attack (if known).
2. Source: Original information source, provide source description, access and assessment of source's reliability.
 3. Chronology: Events since reception of information, including notification of affected unit.
 4. Originator: Identity of individual who initially acquired the information, time information obtained and contacted telephone number(s) to the message sender's command center or watch of message.

ENCLOSURE (5): 24-Hour Emergency Phone Roster

(Thailand Country Code is 66; use when calling from outside Thailand)
(Use full city code, i.e., "02" inside Thailand, when calling from outside Thailand, drop the "0")

Chateau De Bangkok, 29 Soi Ruamrudee 1, Ploenchit Road, Bangkok
1033 Thailand
Telephone: 02-651-4400; Fax 02-651-4500

Somerset Park Suanplu Hotel, 39 Soi Suanplu, South Sathorn Road,
Yannawa, Sathorn, Bangkok 10120, Thailand
Telephone: 02-679-4444; FAX: 02-262-4999

Siam Bayview Hotel Pattaya, 310-2 Beach Road, Cholburi 20150
Telephone: 038-423-8717; Fax: 038-423-8719

Sima Thani Hotel Korat, 2112-12 Mittraphap Road, Korat
Telephone: 044-213-100; Fax: 044-213-121

Lop Buri Inn, Lop Buri, 114 Payothin Street (114 Tanon
Payothin), Lop Buri
Telephone: 36-421-453

JUSMAG-Thailand, Address: POC:
Phone:

U.S. Embassy, 120-122 Wireless Road, Bangkok
Phone: 02-205-4000 (switchboard)
Marine Security Guard: 02-205-4180

MARFORPAC EXECUTIVE AGENT, Camp Smith, Hawaii
Phone: XXX-XXX-XXXX
MARFORPAC EA: Name, Telephone
Alternate: Name, Telephone

MARFORPAC G3 Antiterrorism, Camp Smith, Hawaii
Phone: XXX-XXX-XXXX
MARFORPAC ATO: Name, Telephone
Alternate AT: Name, Telephone

Bumrungrad Hospital,
Phone: 02-667-1175

Thailand Emergency Telephone Number: 191
Thailand Tourist Police

ENCLOSURE (6): JS Guide 5260

Antiterrorism Individual Protective Measures

HOW YOU CAN FOIL TERRORISTS

CJCS PC OCT 2001

**GUARD INFORMATION
MAINTAIN A LOW PROFILE**

- ¶ Destroy all items that show your name, rank, or other personal information.
- ¶ Instruct your family and associates not to provide strangers with information about you or your family.
- ¶ Be cautious about giving out information regarding family travel plans or security measures and procedures.
- ¶ Consider removing your name and rank on your home/military quarters.
- ¶ Avoid the use of your name and rank on answering machines.

TELEPHONE SECURITY

If you receive a threatening phone call or Bomb Threat, report the call to local authorities immediately.

HOME SECURITY

Be Prepared for the Unexpected

- ¶ Brief family members on your residential security and safety procedures.
- ¶ Ensure family members learn a duress word and it is on file at your office.
- ¶ Advise associates or family members of your destination and anticipated time of arrival.
- ¶ Use peephole viewers before you open the door.
- ¶ Don't open the door to anyone until you know who it is.
- ¶ Ensure sufficient illumination exists around your residence.
- ¶ Be alert to strangers who are on government property for no apparent reason.
- ¶ Refuse to meet with strangers outside your work place.

MAIL BOMB INCIDENTS

Be Prepared for the Unexpected

- ¶ Avoid opening or processing mail in close proximity to others.
- ¶ Check mail and packages for:
 - † Unusual odors (shoe polish or almond smell).
 - † Too much wrapping.
 - † Bulges, bumps, or odd shapes.
 - † No return address or unfamiliar return address.
 - † Differing return address/postmark.
 - † Incorrect spelling or poor typing.
 - † Items sent "registered" or marked "personal."
 - † Protruding wires or strings.
 - † Unusually light or heavy packages.
 - † Excessive amount of postage.
 - † Oily stains on the package.
 - † Foreign appearing handwriting.
- ¶ Clear the area immediately; notify your chain of command, local authorities, or FBI.

TERRORISTS DEPEND ON YOU!

A dynamic threat environment demands our utmost vigilance and discipline. We must refine existing protective measures to prevent or substantially mitigate any threat.

This card offers a number of proven security techniques and considerations that limit opportunities to be targeted by terrorists.

GENERAL SECURITY ISSUES

Guard Information About Yourself and What You Do

- ¶ Limit discussion and accessibility of any information (written or verbal) that may provide terrorists insights for targeting.
- ¶ Always use secure means when passing sensitive information.
- ¶ Destroy identifiable information.

Recognize and Report Unusual or Suspicious Behavior

You are the first line of defense against terrorism. Be aware of your surroundings. Write down license numbers of suspicious vehicles; note description of occupants. Report anything unusual to your chain of command, local authorities or the FBI.

Be Prepared for the Unexpected

Plan for the range of threat possibilities; avoid established or predictable patterns.

**TO/FROM WORK
IN TRANSIT SECURITY**

Be Prepared for the Unexpected

- ¶ Look for tampering. Look under and around your auto.
- ¶ At all times, keep your doors locked and windows rolled up.
- ¶ Alter routes and avoid choke points.
- ¶ Alternate parking places.
- ¶ Plan safe locations along your route.

Guard Information About Yourself

Maintain a Low Profile

- ¶ Consider wearing civilian clothing when riding on mass transit.
- ¶ Avoid car markings that identify you as senior ranking DoD personnel (such as GO stars on vehicles).
- ¶ Always remove base stickers if you are selling or disposing of your POV.

**OFFICIAL/UNOFFICIAL
TRAVEL SECURITY**

Be Prepared for the Unexpected

Prior to Travel:

- † Ensure your Level 1 AT Training is current.
- † OCONUS - Receive AOR specific Threat Briefing (by security officer).
- ¶ Select an inside hotel room (away from the street-side window), preferably on the 4th-10th floors.
- ¶ OCONUS - Know the location of the US Embassy and other safe locations where you can find refuge or assistance.

Guard Information About Yourself

Maintain a Low Profile

- ¶ Avoid use of rank or military addresses on tickets, travel documents or hotel reservations.
- ¶ When possible, travel on tourist passports.

NAVMC 3500.103
27 OCT 2010

APPENDIX I

INDIVIDUAL AT PLAN CHECKLIST

TRAVELER(S) DATA

- Rank and Name
- Destination and Dates of Travel

SUMMARY

- Rank/Name has completed Level (state level) AT training in the past 12 months.
- State current terrorism threat level
- State current criminal threat level
- State current FPCON level
- Buddy rule is/is not in effect?
- SECSTATE public announcements or travel warnings?
- Command travel restrictions? If one exists:
 1. Has first O-7 in chain of command designated the travel mission essential?
 2. Has permission to travel been granted by headquarters?
 3. DTG of message?
 4. How will requirements of the travel restriction be met by traveler(s)?
- Indicate AT/FP responsibility

TRANSPORTATION PLANS

- Air Travel (Is air carrier a US Flag carrier and on the FAA approved list?)
- Transportation after arrival at airport
- Intra-area travel

SECURITY

- Weapons? (If weapons are authorized, who will be armed?)
- Workplace security? (MPs, direct hire, contract security, or local police available?)
- Billeting (Hotel security, local police available? List hotel/billeting phone #'s)

MEDICAL

- Does plan state whether/where comprehensive medical care and ambulance services are available?
- Emergency medical support (Is medical information available to traveler?)
- Information/web site info available to traveler(s) regarding vaccinations and Centers for Disease Control?

COMMUNICATIONS

- Availability of telephones in country (public/other) listed?
- Emergency telephone numbers included?
- Contact phone numbers in country (American embassy/consulate, US military, MPs, local police and fire, etc)
- Contact numbers for use as an alternative source for obtaining threat information

AMERICAN EMBASSY/CONSULATE LOCATIONS

- Street address and any other pertinent directions to nearest American Embassy or Consulate (www.usembassy.gov)

EMERGENCY ACTION PLANS

- Evacuation plans (Have emergency telephone numbers and points of contact to change airplane reservations, if required, been provided?)
- Detail reporting procedures for suspicious activity (hotel security, local police, MPs, etc)
- Does the plan indicate locations of safe havens?
- Does the plan address actions to take in the event of:
 1. Terrorist attack on hotel
 2. Terrorist attack against workplace
 3. Mob violence or civil disturbance
 4. New terrorist threat information, change in threat level or FPCON
 5. Natural disaster

PERSONNEL RECOVERY

- Validation that SERE 100 Code of Conduct Level B training has been completed
- Validation that ISOPREP data for all traveler(s) is stored in the Personnel Recovery Management System (PRMS)
- HQ Personnel Recovery/SERE 100 Code of Conduct POC info provided?
- Date SERE 100 Code of Conduct Level B training was complete
- Date personnel recovery data was validated

PROTECTIVE MEASURES

- Protective measure attachments provided to traveler(s)?

APPENDIX J

SAMPLE INDIVIDUAL AT PLAN

Traveler(s): JOHN SMITH.

Destination(s)/Dates: CITY, COUNTRY 080805-080518

1. Summary.

a. City, Country

(1) Terrorist Threat Level: HIGH

(2) Criminal Threat Level: HIGH

(3) Force Protection Condition: LEVEL

b. Buddy rule is in effect. I will be traveling with Jane Doe and John Doe as well as 5 other civilians. John Smith was assigned to the US Embassy in Country and is familiar with the area. We will be traveling together in a group or two smaller groups at all times.

c. SECSTATE Public Announcements or Travel Warnings: N/A

d. CDR, USPACOM Travel Restrictions:

(1) The cities of City, City and the City region are FPCON LEVEL and CDR USPACOM Travel Restricted. The following Provinces are at FPCON LEVEL and CDR USPACOM Travel Restricted, Province, Province, Province (with the exception of Province region), and Province, all of the Provinces, and all of Province.

(2) Requesting Travel permission from HQ USPACOM/J02 before travelling.

(3) State that the travel has been designated "mission-essential" by traveler(s) chain of command, (Include name and rank of person in chain of command that made that designation).

e. AT/FP responsibility: (State whether CDR, USPACOM or Chief of Mission (COM) has FP responsibility, based on DoS/DoD MOAs).

2. Transportation Plans.

a. Air: We will be traveling XYZ Airline from to/from City, Country.

b. After arrival to billeting: We will be transported/escorted by John Smith finance family to our place of residence.

c. Intra-area: We will utilize Individual Protective Measures identified in Attachment 2.

3. Security (responsibility and measures).

a. Weapons: No weapons authorized

b. Workplace: N/A

c. Billeting: No. #, Area, City Zip code (PH): ###-##-##-###-####

4. Medical.

a. Local Hospital/ Services.

1.) HOSPITAL I

Doctor. City

Ph.: (###) ###-####

Emergency: 24hrs service: #####/#####

This hospital is the closest to the Hotel and the Convention Center. It has a small emergency room and ICU. 110 beds. Doctor coverage is spotty. Should only be used in an emergency as the closest hospital. Hospital Service A was recently opened as a joint venture between a City, Australia-based healthcare company and Hospital Assistance, a European medical assistance company in competition with Hospital Service A. This clinic is smaller than Hospital Service A but offers the same services plus an option to schedule a telemedicine appointment with a consultant in City. Hospital I and Hospital Service A offer the best alternatives for primary and emergency medical care outside the U.S. Embassy Medical Unit.

2.) HOSPITAL II

Doctor

City

Ph.: (###) #####
Emergency: ###-####

Hospital II was organized as a clinic oriented to providing care to the expatriate community. It is affiliated with Hospital Assistance, a regional medical evacuation organization. They have a doctor and ambulance on duty 24 hours a day. As in all Country health care facilities, only Country doctors are allowed to treat patients. Hospital Service A, however, has an expatriate consultant physician on the premises most of the time. There is a better chance that this consultant will be involved with your care if the Embassy Medical Unit or Duty Medical Officer calls ahead of your visit.

c. Vaccines. Medical records and vaccines are up to date. No necessary vaccines needed for travel to City, Country.

5. Communications.

a. Availability of telephones in-country: My contact number will be ###-##-####-#####. In addition, two (2) world-quad band cell phones (in which John Smith will be purchasing pre-paid cards) will be provided for the duration of our stay.

b. Contact numbers in country: embassyemailaddress

(1) American Embassy phone numbers: (##)(##) ####-####
AmEmbassy Doctor: Dr. John Doe x####

(2) US military, police phone numbers: Marine Guard Post-
(##)(##) ####-####/####

(3) Local police, fire, etc. phone numbers: (##)(##)
###-####, (##)(##) ###-####, (##)(##) ###-####

(4) Contact numbers for use as alternate sources of obtaining threat information:

(a) USPACOM JOC Director: ###-###-####

(b) JIOC Senior Watch Officer: ###-###-####

6. AMEMBASSY Locations.

(##)(##) ####-####

Address No. #
City, Zip code

7. Emergency Action Plans.

a. Contact the U.S. Embassy Post One (##)(##)####-####/#### and adhere to the guidance provided by the officer of the day, 24hr Duty Officer (##)(##)###-####.

.To change Airline reservations in case of Emergency:
XYZ Airlines: US #-###-###-#### Country (##) ####-####
City - Airport: (##)(##) ###-####/####

b. Upon identification of suspicious activity possibly endangering personnel, facilities, or residences, we will notify hotel security and the local police. Subsequent notification will be made to the American Embassy/Consulate and, if warranted, the USPACOM JOC Director at (###) ###-####.

c. Safe Havens: Embassy for all threats other than those to the embassy. For threats to Embassy, we will remain in the residence unless otherwise instructed by Embassy personnel.

8. Specific Contingency Plans.

a. Terrorist attack on Embassy: cease activities; return to hotel room or any other available safe haven; assess situation; contact USPACOM JOC Director at (###) ###-#### for guidance.

b. Terrorist attack against workplace: cease activities; evacuate to Embassy and contact USPACOM JOC Director at (###) ###-#### for guidance. Continue to assess situation, and plan to evacuate via airlines. Host nation security and law enforcement personnel increase security of workplace and embassy until situation is resolved, or depart country.

c. Mob violence or coup: cease activities; remain at hotel until situation is resolved; coordinate with Embassy and depart via air.

d. In the event a terrorist attack occurs in country, new terrorist threat information is received, change in Threat Level or FPCON: coordinate with Embassy/USDR; assess situation; contact USPACOM JOC Director at (###) ###-#### and parent unit,

and either continue with enhanced Embassy/host nation security,
or cease activities and depart country via air.

9. Personnel Recovery.

a. ISOPREP data is filed with the XYZ-### X-# Security
Office.

b. HQ USPACOM J35 Personnel Recovery POC:

Mr. John Doe, USPACOM PR Analyst
SIPRNET E-mail: webaddress
NIPRNET E-mail: webaddress
Phone: ###-####

c. Personnel Recovery data validated on: (Enter date
validated). webaddress

10. Protective Measures. Traveler(s) will comply with
attachments 1 and 2 and the FPCON measures in Instruction
####.#X.

11. Approval. In accordance with Instruction ####.#X this FP
Plan is approved.

(APPROVER'S NAME)
(RANK, BRANCH)
(Title, Section)

Attachments:

1. Preparation and Planning
2. Antiterrorism Individual Protective Measures

**Antiterrorism Plan Attachment 1
Preparation and Planning**

1. AT training, intelligence and threat briefings

a. Travelers have completed Level I AT Awareness training in the past 12 months.

b. Travelers have received a threat briefing for the destination(s) in the past 3 months that included information on:

(1) Historical activity

(2) Recent activity

(3) Known groups

c. Traveler will wear civilian clothing while traveling.

d. Safety advisory: Traveler has been provided safety/security advisories, with emphasis on hotel/street crime, fire safety, medical tips, water/food safety, and related topics.

e. Security advisory: Traveler has reviewed information on safety and security.

f. Crime advisory: Traveler will safeguard valuables and take advantage of any provided safes. Traveler will remain alert and take the same precautions he would take in any major urban area. Petty criminals are most active in predominately tourist areas, airports, markets, restaurants, public transportation and hotels.

2. Emergency Action Plan:

a. Communications: Traveler has been provided with emergency telephone numbers.

b. Evacuation plans: No requirement to evacuate the country is anticipated; however, traveler will have telephone numbers and points of contact to change airplane reservations if required.

c. Upon identification of suspicious activity possibly endangering personnel, facilities, or residences, traveler will notify hotel security, local police, MP's or MI as appropriate. If warranted, subsequent notification will be made to the USPACOM CDO at ###-###-####.

d. Safe Havens: Traveler will proceed to nearby US Government facilities or remain in hotel unless otherwise instructed

3. Specific contingency plans:

a. Terrorist attack on hotel:

- (1) Contact appropriate US Government security facility
- (2) Then evacuate to nearest US Government facility

b. Terrorist attack against workplace:

- (1) Follow instructions of visited workplace.
- (2) Assess situation, and plan to evacuate via airlines.

c. Mob violence or civil disturbance:

- (1) Monitor situation
- (2) If off-duty, cease activities
- (3) Remain at hotel until situation is resolved
- (4) Coordinate with appropriate US Government facility and depart via air if necessary.

d. New terrorist threat information, change in Threat Level or FPCON:

- (1) Coordinate with appropriate US Government security facility
- (2) Assess situation, contact home unit
- (3) Continue with enhanced security or cancel visit and depart via air.

- e. Natural disaster in AO:
 - (1) Assess situation
 - (2) Coordinate with visited workplace
 - (3) Cancel meeting if appropriate
 - (4) Contact home unit and depart via commercial air if appropriate.
 - (5) If disaster is of such magnitude air flights unavailable, coordinate with appropriate US Government security facility to depart via other airports.

Antiterrorism Plan Attachment 2
Antiterrorism Individual Protective Measures

Vary

- Routines
- Schedules/times
- Travel routes
- Eating establishments
- Shopping locations
- Attire

Avoid

- Crowded areas, demonstrations, public holiday festivals, known trouble spots
- Excessive use of alcohol
- Offensive, insulting, illegal, or unethical behavior

Know

- How to use local telephone systems and have correct change
- Where the US Embassy is (address and telephone number)
- Where the nearest police/fire stations are
- Where the nearest hospital is
- Where friendly/allied foreign embassies/ consulates are
- Where safe havens are
- Where your hotel/billeting site is in relation to everything else
- Simple phrases in the predominant language of the country you're visiting

Bomb Incidents

- Be alert to suspicious objects found
- around workplace sites, hotel, airport, or transportation -
- Unattended baggage
- Unattended briefcases
- Unattended boxes, crates, musical instrument cases

Unattended vehicles

- If a suspected bomb is discovered,
- Clear the area immediately
- Notify local security, and your chain of command

Recognize potential letter/package bombs by

- Unusual odors

- Excess postage
- Specifically addressed to an individual or the entity's senior officer/person
- Bulges, bumps, or odd shapes
- No return (or unrecognized) address
- Protruding wires/strings
- Poor spelling, punctuation, excessive markings (e.g., Eyes Only, Personal, Confidential)
- If discovered, evacuate area, call security; DO NOT move or touch package

Travel Security

Airport terminals

- Use "sanitized" (NO USG affiliation) or concealed bag tags
- Minimize time in terminals; wait in sterile areas
- Refuse to carry luggage for strangers; report requests to airport authorities
- Watch other waiting passengers; be alert to nervous, suspicious characters

At hotels

- Do not give room number to strangers
- Request a room facing away from the street, between the 4th and 7th floors
- Use curtains
- Leave a light or TV on; give the appearance of occupancy; use "do not disturb" door sign
- Answer telephone "hello"; be circumspect in your conversations

Domicile to duty

- Use alternate parking places
- Lock unattended vehicles
- Look for tampering; fingerprints, grease marks, dirt smudges, or specifically cleaned areas
- Alter routes and times
- Plan escape routes as you drive
- Be alert to following/approaching mopeds/ cycles
- Do not pick up hitchhikers
- Drive with windows up and doors locked
- Avoid chokepoints
- Keep vehicle gas tank at least half full; maintain vehicle well

APPENDIX K

INSTALLATION EMERGENCY RESPONSE PRIORITY PLANNING TEMPLATE

1. Situation. An installation may experience an incident(s) that either exceed or have the potential to exhaust the installation's emergency response and resource capabilities over multiple operational periods. As part of the Installation Emergency Management Plan, emergency response priorities must be established to optimize response efficiency and effectiveness with regards to limited resources. In addition, response priorities have to be established to consider not only life saving activities, but also the maintenance of missions and operations at the installation. The purpose of this enclosure is to provide emergency response order of priority that takes into consideration both life saving priorities and the need to maintain the operational posture of Host and Tenant Command Task Critical Assets (TCAs) and the Supporting Critical Infrastructure Critical Assets (SICAs).

2. Emergency Response Priorities. In any emergency situation, the installation emergency response will be guided by the following overarching priorities:

a. Priority One - Personnel. The highest priority is the safety and well-being of those who live, work, and visit the installation.

b. Priority Two - TCA and SICA. Serious incidents involving these critical assets have significant mission impact for the installation and its tenants. Emergency response to mitigate and limit the damage to these assets is essential to ensure continuity of operations. Emergency response priorities must be established for these critical assets once life-saving activities have been accomplished. Emergency Dispatch and First Responders need to have the list of these assets and/or the facilities that these assets are located available to assist in prioritizing their emergency response. TCA and SICA priority response shall further be broken down into:

Priority Response 2 (a) - Tier I Critical Assets
Priority Response 2 (b) - Tier II Critical Assets
Priority Response 2 (c) - Tier III Critical Assets
Priority Response 2 (d) - Tier IV Critical Assets

c. Priority Three - High Occupancy Facilities. Where not already covered by Personnel Response Priorities, these

facilities include but are not limited to; barracks, maintenance facilities, hospitals/clinics, training classroom buildings, theaters/auditoriums, arenas and special event venues, commissary, exchange, restaurants, and child care facilities.

d. Priority Four - Unoccupied Facilities. Unoccupied offices, warehouse buildings, and other facilities.

3. Tasks/Responsibilities

a. Installation Emergency Management Working Group (IEMWG)

(1) Develop emergency response priorities/checklists that support paragraph 2 priorities above. Incorporate those priorities in any automated system that assists or directs response in support of the various response types.

(2) Conduct training for appropriate Incident Commanders, emergency dispatch personnel, and first responders and when appropriate, local, regional, State and Federal partners on the response priorities. Document this training in accordance with appropriate training policies.

(3) Coordinate with local, regional, State, and Federal emergency response agencies to facilitate development of mutual emergency response support agreements in the form of Memorandums of Agreement/Understanding (MOA or MOU), Mutual Aid Agreements (MAA), and Inter-Service Support Agreements (ISSA).

(4) IEMWG may be combined with other Mission Assurance Working Groups, (i.e. AT/CBRNE/CIP).

b. Installation Critical Infrastructure Program (CIP) Officer.

(1) Coordinate with the Installation Emergency Manager to implement mission critical assets and supporting infrastructure critical assets into the emergency response priority list.

(2) Coordinate with the Installation Exercise & Evaluation Team (IEET) to plan and execute any discussion based, tabletop, functional and full-scale exercises that incorporate CIP injects. These injects must exercise incidents involving mission critical assets and supporting infrastructure critical

assets, to include verification of emergency response priorities.

(3) Provide support to the Emergency Operations Center operations as required during for each incident.

(4) Collaborate and coordinate with local, regional, state, and federal agencies to facilitate development of mutual emergency response support agreements.

APPENDIX L

SAMPLE DESIGN BASIS THREAT

Possible Areas of Exploitation

The list below highlights the potential planning considerations that a terrorist group might consider when studying Marine Corps Installation XYZ. Although there is no evidence to suggest any terrorist group active in the State or the United States has the capability to replicate the 9/11 style of coordinated attack, law enforcement and security officials continue to uncover evidence of domestic and foreign plans to execute attacks on U.S. soil. Moreover, a simple bombing that inflicts numerous casualties or impedes base operations requires little expertise, training, or sophistication, yet provides a significant political and publicity reward to the perpetrators or their affiliated groups. Additionally, the most sophisticated and committed terrorists are more concerned about achieving success than surviving the operation. Therefore, they prefer to abort and/or attack a secondary objective if it appears likely the attack on the primary target will fail.

Most American terrorist groups place a high priority on personal survival and are the most easily deterred by changes in security patterns. Whether American or foreign, suicidal or survival-based in their thinking, terrorists often attack a nearby target in cases where the security at the primary target reduces the chances of success; thus the strike on a less well protected nearby target in ways that will affect the primary target.

Suicide Bombing

Suicide bombs are a deadly and highly effective terrorist tactic. The 9/11 attack is the only terrorist suicide attack ever conducted in the United States. Although not the case with the 9/11 attack, suicide bombings are typically launched from a staging area close to the target (usually within 5km for a vehicle, 3km for a pedestrian). There is very little likelihood of Installation XYZ suffering a foot pedestrian-based suicide bombing. However, terrorists may consider placing a bomb inside a vehicle, with or without the driver's knowledge.

Car Bombing

Over the past decade there have been no recorded incidences of a suicide bomber walking/hiking more than 3 km to the intended target. The odds of a terrorist or group of terrorists hiking through the terrain surrounding Installation XYZ is low. It is

more likely that a group would use vehicles to convey explosives on base. However, it is possible that terrorists may place timed or remote detonation explosives on base-approved vehicles while those vehicles are outside Installation XYZ (as was done by a German terrorist group in the Ramstein Air Base bombing of 1981). Most vulnerable would be Marines/spouses/base employees who live off-base in one of the surrounding towns.

Impact: Depending upon the number of vehicles used in the attack, effects could range from a single incident killing or wounding a small number of victims to a coordinated attack hitting multiple base locations simultaneously. Beyond casualties, the attacks could do considerable damage to buildings or other key facilities, have a high psychological impact, generate significant publicity, and severely hamper ingress and egress to the base for several hours after the attack.

Installation XYZ Vehicular Access to Mainside

Potential Areas of Concern:

1. Road Gates

A vehicle able to breach a closed gate or run the checkpoint could deliver an explosive to Mainside.

2. Off-Road Access

Because of the open nature of Installation XYZ, an off-road vehicle can gain access by traversing the desert, then following one of numerous dirt trails back to Mainside.

Headquarters Building

The Installation XYZ Headquarters is located centrally in Mainside. While barricades are present to block off parking areas on the NW and SE sides of the HQ building, an attack could occur if the barriers are not fully closed. A car, van, or cargo truck could potentially deliver an explosive attack against the building. A terrorist would likely consider 6 possible tactics:

- 1. Smuggle explosives onto the vehicle in luggage through the Main Gate to detonate at the HQ entrance.**

2. Smuggle explosives on his/her person through the Main Gate to detonate either outside the building, or attempt to get into the building before detonation.
3. Attach explosives to the vehicle undercarriage while it is outside the base, and use a timed, remote, or GPS-triggered detonator.
4. Use a cargo truck hauling a fertilizer bomb or plastic explosives to crash the gate and make a run for the building.
5. Use an off-road vehicle to access the base from the NE and enter the base road system.
6. Detonate explosives at the Main Gate if it appears they cannot deliver them onto the base.

Impact: A deliberate attack in this area has the potential for inflicting casualties (including senior base leadership) and hampering base operations.

Blast from 5000lb Vehicle Bomb - Plastic Explosive - CCHP Plant

Running 24/7 (except for two weeks yearly of maintenance downtime), the turbine burns about 50,000 therms of natural gas monthly. Although rated for 7.3 MW, the output actually comes to around 7 MW because of combustion inefficiencies at higher elevations. Fuel consumption and power output are also turned down slightly in the lowest-load winter periods, in order to maximize efficiency.

After yielding up its electricity, the turbine's hot exhaust is captured in a heat-recovery generator to supply heat for roughly a third of the base's central heating plant; this consists of three international boilers outputting 40 million Btu/hr. apiece. The Taurus actually was sized "in order to supply heat for one of those boilers," says Morris, because boiler load is a prime scaling factor in many cogeneration (cogen) projects. "Whatever amount of [exhaust] heat you can use, and not waste your gas producing it," he says, will tend to determine the appropriate turbine. During high desert winters, which are sometimes mild and short, two boilers typically might be running, but in the summertime, their gas valves are closed because the base's hot-water needs can be supplied largely by the Taurus' exhaust—to the tune of 30-35 MBtu/hr.—as planned.

- This hot-water output is then pumped through about 40 or 50 mi. of piping, at up to 2,400 gal./min., to supply 80% of Marine-base buildings "with very-high-temperature hot water

for domestic use, some steam applications, and building heating," notes Morris.

- All of the boilers and the Taurus genset can be fired with either natural gas or diesel as a backup.
- The array includes 8,706 solar panels, each capable of yielding 150 W, or 1.2 MW total. The system uses single-axis tracking, which feeds into five inverters and then into five transformers and into a main line that carries it into the cogen plant.
- SCE's grid enters the base from a 34.5-kV main and a 12.47-kV secondary feed, serving one section of buildings. The cogen and PV feed into the latter via four main breakers.

Impact: An attack on the combined cooling, heating, and power (CCHP) plant could reduce power to Installation XYZ and hinder operations. A multiple target attack could render the base powerless if the terrorists were to strike the plant along with off-base energy delivery lines.

Distribution of Natural Gas

The gas company provides natural gas for many portions of Installation XYZ. Service is provided to approximately 3,000 properties.

One six-inch, high-pressure (400 psi) main feeds the community, entering the city (west to east) along the north side of the highway. The movement is then north along XYZ Avenue, east along XYZ Drive to XYZ Avenue, north along XYZ Avenue to XYZ Road, then north to Installation XYZ.

Three regulator stations are included in the local distribution network, two in the city and one on Installation XYZ. The six-inch main feeds into the regulator stations, the pressure is reduced to approximately 45 psi, and natural gas is distributed to the customer. The South Regulator is located near the southwest corner of XYZ Drive and XYZ Avenue, and feeds service to most of the southern portion of the city. The North Regulator station is located northeast of the intersection of XYZ Road and XYZ Road. It provides service to the northern portion of the city. From the North Regulator, the main goes north to Installation XYZ, providing service to the Base. A regulator station, from which service is distributed, is located at the main terminus on Installation XYZ.

Source: <http://www.website.html>

Blast From 5000lb Vehicle Bomb - Plastic Explosive - Naval Hospital

A direct attack against the Naval Hospital would not only cause casualties but also render Installation XYZ at least partially incapable of dealing with the victims of the attack. Regimental and Battalion Aid Stations can provide immediate first aid to any casualties. Casualties requiring medical attention would need to be transported to hospitals in the city, approximately 60 miles by vehicle or 40 miles by airlift.

Blast From 5000lb Vehicle Bomb - Plastic Explosive - NH Power Generators

An attack on the power supply for the hospital may be more effective for denying the use of the hospital to Installation XYZ. No data were available on any back-up supplies or emergency generators.

Source: <http://website.pdf>

Blast From 5000lb Vehicle Bomb - Plastic Explosive - Mess Hall

An attack against one of the mess halls during peak dining times could cause mass casualties. The mess halls appear to be accessible for a vehicle-borne explosive attack. Concrete barricades in front of the hall could provide some protection to the dining portion of the hall.

Air Attack via Aircraft Hijacking

It is possible that an individual or group could (a) hijack an airliner on approach to Installation XYZ, or b) hijack or pilot a small aircraft at a smaller airport with the intent of attacking base facilities.

1. **Air:** Air attacks can occur in two ways:

- **Least Likely But Most Damaging:** 9/11-style attack, hitting troop barracks or Headquarters buildings.
- **More Likely But Far Less Damaging:** Flying a private plane or remotely piloted aircraft into troop barracks or Headquarters buildings.

Impact: A successful or unsuccessful attack on the base from the air would at least disrupt base operations for several hours. Even if the terrorists failed to cause significant damage, the base would be forced to lock down for inspections and investigations.

Psychological Impact: Regardless of the outcome of the attack, it will have a psychological effect on base personnel and surrounding residents and will hamper base operations. A successful attack could create panic outside of Installation XYZ if fires introduce hazardous materials into the atmosphere, causing evacuations. Evacuations of the base and/or city could potentially inhibit base supply and outside services, as well as create transit problems for off-base officers for 24-72 hours. The long-term political/psychological impact within the area would challenge Installation XYZ's ability to defend itself.

Attack During On-Base Event

Terrorists or anti-military activists may consider entering base events to initiate an attack or incident to generate publicity for their cause. Such attacks are easily discouraged and/or prevented by vigilant security and screening.

Water Treatment Plants

Assessment: Media sources may stress the base's water treatment plants as a viable terrorist target. However, the sheer volume of water processed by the base will dilute and thus negate any attempt to poison or infect the populace. An attack on the sewage treatment plant and distribution system would be more threatening to the base population's health and prove more inconvenient and expensive to overcome or repair.

Impact: The impact of such an attempt would be psychological in nature only. Portable water treatment and local stores on base and in the surrounding area would supply enough water to supplement base usage during the attack's investigation.

Poisoning Fast-Food Supplies

Assessment: Given enough planning and coordination, it is at least possible for a group to introduce foreign agents (biological or chemical) into the consumables meant for the numerous fast-food chains throughout the base. Such an act is highly improbable and no North American terrorist group has ever made such an attempt, but force protection conditions should consider procedures to reduce the possibility of such an attack during high-threat periods.

Impact: If successful, such an attack would render a number of personnel ill and could possibly cause fatalities. The psychological effects would likely be greater than the effects on base personnel. There would also be a considerable economic cost in evaluating the shipping and food storage methods for all on-base fast-food restaurants.

Off-Base Range Attacks

Assessment: An attack from off-base using small arms or man-portable rocketry (RPG) is unlikely to have a large impact on base functioning. Attacks could also occur in other areas, but would not leave a quick escape route.

Base Housing

Impact: The impact of an off-base attack would be minimal. Without breaching what appears to be fencing surrounding base housing on the south end of Mainside, a terrorist would be limited to harassing gunfire or RPG attacks. While the psychological impact could cause problems for the base, the chance for high numbers of casualties is minimal. The possible exception would be an attack on the Community Center (Bldg. XYZ) during peak use times. Housing in the area is similar in nature.

Biological/Chemical Attack

Assessment: The threat from a biological or chemical attack is minimal. It would be extremely difficult to transport the materials needed onto base. An attack staged from off base would require huge amounts of agents in order to avoid dispersal and/or diffusion while traveling onto Installation XYZ. The desert's aridity, temperature, and wind make this type of attack improbable. A better target would be in the town of XYZ to tie

up the command's resources during treatment and clean-up operations.

Impact: Although the loss of life probably would be minimal, a chemical/biological/toxic material incident would draw global media attention and shut down the affected area of the base and highway for several hours. The pollutants would reach the base given sufficient wind, but the potency would be limited by the type of shipment carried, the quantity delivered, and the size of the agent. If successful, it could render a number of personnel ill, with possible fatalities. The media coverage would have a psychological and political impact far beyond Installation XYZ. An attack on the city would inevitably draw media attention to the command. In the long term, attacks on the civilians near the base could bring the citizens to resent having a U.S. military base close by.

C-VAC Note: Media speculation aside, the manufacture and transport of biological and chemical agents is a complex and dangerous task requiring great care. Although many terrorist organizations are pursuing chemical and biological weapons capability, Japan's Aum Shinrikyo is the only terrorist group to have manufactured a chemical agent successfully and transported it to the target. But even after spending \$10 million dollars, Aum Shinrikyo chemists were unable to scale up to industrial production of sarin. Among the more than 9,000 known terrorist attacks worldwide since 1975, only 16 incidents involved chemical or biological weapons. Procuring deadly chemical or biological agents is the first hurdle a terrorist group would have to overcome. Smallpox virus, for example, has been officially stored in only two repositories—one in Atlanta and one in Russia—since the disease was eradicated in 1980. Some U.S. officials suspect that Iraq and North Korea might have held on to some of the virus, but experts say it is so contagious that only the most foolhardy terrorists would risk working with it.

Anthrax also poses problems. It occurs naturally in sick cattle and camels, but isolating a virulent strain that would kill humans is a difficult task. Even assuming a terrorist organization got its hands on a deadly chemical or germ, dispersing them in such a way as to kill large numbers of people would require skills that only a handful of governments have ever mastered. One of the most common fears is that city reservoirs might be poisoned, rendering kitchen taps instruments of death, but experts say the huge amounts of agent that would

have to be dumped in a reservoir to have any effect make this approach impracticable.

APPENDIX M

RISK MANAGEMENT WORKSHEET

OVERVIEW

This risk management worksheet can be used in conjunction with Chapter 3 to understand the antiterrorism (AT) risk management process. It is a useful guide through each step of the risk management process; however, it may not provide as effective analysis as more advanced risk management tools.

Step 1 CRITICALITY ASSESSMENT		
Identify assets that would be targeted as a result of exploiting this vulnerability.		
Asset Name	Impact of Loss	Criticality Rating
Overall Criticality Rating for this Vulnerability:		
Overall Criticality Rating Guidance:		
<p>High — Indicates that compromise to the targeted asset would have grave consequences leading to mass casualty or mission failure; or indicates that a compromise to assets would have serious consequences resulting in loss of life or severe mission degradation</p> <p>Medium — Indicates that a compromise to the assets would have moderate consequences resulting in potential loss of life or severe injury and loss of mission-essential resources that would impair operations for a limited period of time</p> <p>Low — Indicates little or no impact on human life or the continuation of operations</p>		

Step 2 THREAT ASSESSMENT			
Threat Level:	Asset:		
Design Basis Threat	Explosive		
	Ballistic		
	Inertia		
	Direct Fire		
	Indirect Fire		
	Air		
	Sea		
	CBRN		
	Natural Hazards		
Weapons and Tactics that would be used when exploiting this vulnerability		Weapon / Tactic	Priority Level
	1		
	2		
	3		
	4		
	5		
	6		
	7		
	8		
	9		
	10		
Other Threat Contributing Factors:			
Overall Threat Rating for this Vulnerability:			
Overall Threat Rating Guidance:			
<p>High — Indicates that a credible threat exists against the assets based on our knowledge of the adversary's capability and intent to attack the assets, and based on related incidents having taken place at similar facilities; natural hazard - occurs frequently.</p> <p>Medium — Indicates that there is a potential threat to the assets based on the adversary's desire to compromise the assets, and the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents. Indicates there is a significant capability with low or no current intent that may change under specified conditions; natural hazard - occurs annually.</p>			

Low — Indicates little or no credible evidence of capability or intent, with no history of actual or planned threats against the assets.
Source of Threat Information; natural hazard - rarely to never occurs.

Step 3 VULNERABILITY ASSESSMENT

Identify Vulnerability of Asset

Additional Factors that increase or decrease the ability to exploit this vulnerability:

Overall Vulnerability Rating:

Overall Vulnerability Rating Guidance:

High — Indicates that there are no countermeasures, or existing countermeasures are ineffective or easily defeated by an adversary or natural hazard.

Medium — Indicates that there are countermeasures in place, but at least one weakness exists that some known adversaries or natural hazards would be capable of exploiting.

Low — Indicates that multiple layers of effective countermeasures exist and few or no known adversaries or natural hazards would be capable of exploiting the vulnerability.

Step 5	RISK ANALYSIS
Overall Risk Rating for Asset:	
Overall Risk Rating Justification:	
Risk Rating Guidance: The Overall Risk Rating is based on the four elements above. Enter a rating of High (H) - Medium (M) - Low (L) for the Overall Risk Rating. If the Overall Risk Rating is noticeably different than the threat, vulnerability, asset criticality, and AT/FP plan effectiveness, explain the reason for the difference in the justification section above. For example if Threat = High, Vulnerability = High, Criticality = Medium, and AT/FP Plan Effectiveness = Low, and the Overall Risk Rating = Low, the Overall Risk Rating does not reflect the ratings of the individual components, and therefore must be explained.	
Risk Acceptance Justification:	
Impact if not Addressed:	

Step 6		RISK MITIGATION	
Procedural Recommendations			
Recommendation 1.			
Development Requirements:			
Impact of Implementation:			
Time Required to Implement:		Residual Risk:	
Other Vulnerabilities Affected:			
Recommendation 2.			
Development Requirements:			
Impact of Implementation:			
Time Required to Implement:		Residual Risk:	
Other Vulnerabilities Affected:			

Step 7		COUNTERMEASURE STRATEGY	
Resource Recommendations			
Recommendation 1.		Cost:	
Development Requirements:			
Impact of Implementation:			
Time Required to Implement:		Residual Risk:	
Other Vulnerabilities Affected:			
Recommendation 2.		Cost:	
Development Requirements:			
Impact of Implementation:			
Time required to Implement:		Residual Risk:	
Other Vulnerabilities Affected:			

APPENDIX N

SAMPLE LOCAL VULNERABILITY ASSESSMENT

CLASSIFICATION

SUBJECT: LOCAL VULNERABILITY ASSESSMENT

(U) **SCOPE**

(U) This Local Vulnerability Assessment (LVA) supports the 2010 Marine Corps Missin Assurance Assessment Program (MCMAAP). As per reference (a) it states "Local Commanders shall conduct a Local Vulnerability Assessment for facilities, installations, and operating areas within their area of responsibility. The Local Vulnerability Assessment shall address the broad range of physical threats to the security of personnel and assets and shall be conducted at least annually."

(U) The scope of this LVA will encompass AT Plans and Programs, Counterintelligence, Law Enforcement Liaison, and Intelligence Support, AT Physical Security Measures, Vulnerability to a Threat and Terrorist incident response measures, and Terrorists' use of WMD.

- (U) AT Plans and Programs shall examine _____ AT program and its ability to accomplish appropriate standards contained in reference (x) and those established by Higher Headquarters.
- (U) Counterintelligence, Law Enforcement Liaison, and Intelligence Support shall focus on the installation's ability to receive threat information and warnings from HHQ and local resources. The ability to process and disseminate such information will also be assessed.
- (U) AT Physical Security Measures will be assessed to determine the Installation's ability to protect personnel by detecting or deterring terrorist or criminal acts and failing that, to protect by delaying or defending against those acts. Operation Security (OPSEC), the Critical Infrastructure Program, and food protection will also be assessed here.
- (U) Vulnerability to a Threat a Terrorist Incident Response Measures will be examined to determine the installation's ability to determine its vulnerabilities against commonly used terrorist

weapons and explosive devices, structural or infrastructure's ability to withstand terrorist events, and their ability to respond to a terrorist event emphasizing on mass casualty situations.

- (U) Terrorists use of WMD will be examined to determine the installation's vulnerability to use of WMD and CBRNE.

(U) In accordance with reference (x) the _____ All-Hazards Working Group will prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities, and report to the _____ commander within 90 days. Further, the findings within the LVA will be populated within the Core Vulnerability Assessment Management Program (CVAMP).

(U) Marine Corps Police Department provides Law Enforcement (LE) and Military Working Dogs (MWD) to secure installation. There are multiple LE and MWD posts or patrols in and around _____ and are posted 24/7.

Assumptions:

- a. Terrorist, criminal, and other assumptions pertaining to installations are placed here

(U) **AREA CHARACTERIZATION**

This section should provide an overview of location, terrain, climate, installation information, roadway systems, and access control information for installation.

(U) **EXECUTIVE SUMMARY**

This section details the importance/use of the installation for the U.S. Marine Corps, installation sites, population (military, civilian, contractor), and other important facts.

(U) Likelihood of Attack (Threat Analysis)

Overview of information pertaining to possible attack based on federal, state, and local authorities.

(U) Friendly Forces

Overview of federal, state, and local authorities, as well as military forces, operating in/around installation. Also list agencies that could assist the installation during an emergency.

(U) Risk Assessment

Standard 3,4,5, and 6 of DoDI 2000.16 provides guidance for determining terrorism threat and risk assessments based on four elements: terrorist threat, vulnerability of facilities, terrorists' ability to conduct activities and mitigation measures already in place. The Criticality and Vulnerability (CV) rating and the Risk Assessment level for _____ is at "level."

Security and Mitigation Effectiveness (Current Security System)

This may be the first classified statement here. You need to assess the security forces capability, equipment, and training as it relates to what they bring to the table. Remember to look at their manning of posts and what their ATRP awareness is as a whole. As such, the existing security system effectiveness in preventing adversaries from committing acts of terror or crime is rated high/medium/low/non-existent.

ALL HAZARDS THREAT ASSESSMENT (Should be Classified)

NCIS Threat Assessment: Entire NCIS assessment here.

Civil Disturbance: Likelihood of disturbances from federal, state, local assessments placed here.

Crime: Department of Justice and other federal, state, and local assessment information is placed here.

Medical/Health/Safety Threat: Information from medical clinic officials.

Hazard generally refers to unintentional incidents such as accidents, events of nature such as destructive weather, and equipment failure that cause loss or damage to assets or personnel.

Toxic Industrial Chemicals (TICs)/Toxic Industrial Materials (TIMs) and locations of activities that produce biohazards (i.e. hospitals and medical research facilities) should be included in the Hazard Assessment.

CRITICALITY ASSESSMENT

(U) Insert an overview of the installation's Mission and Critical Infrastructure programs.

Objective: Number of CAs addressed in assessment. All Tier I-III critical assets must be addressed.

Considerations: The Critical Assets lists should be considered when planning for security activities during increased threat periods, and for prioritizing funding for facility improvements. (Insert lists below paragraph)

RISK ASSESSMENT

After completing the threat, vulnerability, and criticality assessments, a determination has to be made to assess overall risk (review risk management procedures). Utilize pictures and requirements to state your case to the commander. Each critical asset/program/plan/deficiency should be assessed individually utilizing the criteria below:

1. List CA/Program/Plan/Deficiency assessed
2. Observations
3. Recommended Mitigation Measures
4. Commanders Risk Acceptance Response (Yes/No)

APPENDIX O

ASSESSMENT MITIGATION PLAN / GO/FO Letter

SSIC
ATO
dd Mmm YY

CLASSIFICATION

From: Commanding Officer, Marine Corps Base/Station XXXXX
To: Commander, Marine Corps Bases, (location)
Subj: MARINE CORPS BASE/STATION XXXXX ASSESSMENT MITIGATION
PLAN (U)

Ref: (a) DoDINST 2000.16

1. (U) XXX Team x conducted an assessment of MCB/S XXXXX, (location), from 29-31 February 20XX.
2. (U) Per reference (a), the following were identified by the XXXX team and have been prioritized with corresponding actions to mitigate or eliminate the identified risk:
 - a. (c) Entry Control Points lack required AT design features.
 - (1) (c) The Main Gate construction project was under renovation during the assessment. The installation of the final denial barriers was completed on dd Mmm YY.
 - (2) (c) A temporary barrier was placed to mitigate reverse entry via the Main Gate outbound lane until the project is completed. Estimated completion date (ECD) is dd Mmm YY.
 - b. (c) Exploitable entry control and search procedures.
 - (1) (c) A background check on all contractors is validated by the Law Enforcement Operations Center, to include screening names against the debarment list, prior to issuing passes.
 - (2) (c) An additional member of the Auxiliary Security Force was added to maintain control of occupants as an overwatch.
 - (3) (c) The use of military working dogs has been increased at all gates.

(4) (c) The Provost Marshal Office (PMO) is revising standard operating procedures (SOP) for gate operations. ECD is dd Mmm YY.

c. (U) Inadequate facility standoff.

(1) (c) There is limited parking on the Base/Station and future expansion will further limit parking.

(2) (c) The Facilities Department has developed a plan to incrementally increase standoff distances. The Antiterrorism Officer (ATO) will prioritize areas based on the threat, mission essential vulnerable areas, critical infrastructure and high-population areas, and availability of funding. This will be a multi-year project due to ongoing construction. MCB/S XXXXX will continue to mitigate the threat until the situation is resolved. ECD: 20XX.

d. (c) Building XXX is a single point failure.

(1) (c) Post X acts as the alternate Emergency Communications Center. PMO is working the issue to provide a redundant capability.

(2) (c) PMO will submit an unfunded request to the Comptroller for all emergency equipment, working closely with the ATO in an attempt to retrieve funding via Global War On Terrorism funding or Combating Terrorism Initiative Funds.

(3) (c) PMO will coordinate with Marine Corps Property and Ordnance to develop an alternate arming and resupply point until the situation has been resolved. ECD is dd Mmm YY.

3. Point of contact for this matter is Mr. Name, MCB/S ATO at Commercial (###) ###-####, DSN ###-####.

//signed//
Name

Derived from: DTRA SCG VA
Dated XX XXXX
Declassify on: dd Month YY

APPENDIX P

SAMPLE VULNERABILITY MITIGATION REPORT

Vulnerability Mitigation Report								
List	Vulnerability	Rank	Mitigation	Time	Cost	Rank	Commanders Priority	Comments
1	Stand off in front of HQ Building	7	Request Barriers be placed in front of building	1-2 months	Depends on number of available barriers in base stockpiles.	3	2	
			MilCon permanent obstacles in front of building	1 year	\$800,000.00	3	3	
			Shutdown road in front of building	Immediately	Increase traffic on surrounding roads.	5	1	
2								
3								
4								
5								

VULNERABILITY MITIGATION REPORT INSTRUCTIONS

Vulnerability. List all vulnerabilities.

Rank. Rank vulnerabilities based on a scale of 1-10 with 1 as the lowest level of vulnerability and 10 as the highest level of vulnerability. The Commander or ATO must

establish a description for each rank in terms of mission degradation, casualties, damage, etc.

Mitigation. List possible mitigation measures that may reduce the vulnerability rank.

Time. Record the time it will take to implement the mitigation measure.

Cost. Record the costs of implementing the mitigation measure (monetary, manpower, etc.).

Rank. Rank the vulnerabilities according to their evaluation after the mitigation measures are in place. Ranking must comply with the rating scale of 1-10 with 1 as the lowest level of vulnerability and 10 as the highest level of vulnerability.

Commander's Priorities. Assign the order of implementation of the mitigation measures based on the Commander's priority (1 being the first to be implemented, 2 being the second to be implemented, etc.).

Comments. Provide any additional comments or information.