

**FOR OFFICAL USE ONLY (FOUO)**

**DEPARTMENT OF THE ARMY  
HEADQUARTERS III CORPS AND FORT HOOD  
Fort Hood, TX 76544-5056  
30 May 1991**

**FH Reg 525-13**

Military Operations  
**THE FORT HOOD COMBATTING TERRORISM (CBT/T) PROGRAM**

---

**SUMMARY.** This regulation prescribes policy and procedures and assigns responsibilities for the Fort Hood CBT/T program.

**SUPPLEMENTATION.** Supplements to this publication will not supercede, change, rescind, or duplicate higher level command policy. When an addition, change, or deletion is needed, the first consideration will be given to changing the basic document.

**SUGGESTED IMPROVEMENTS.** The proponent for this regulation is the Assistant Chief of Staff (ACofS) G3/PTM. Users are invited to send comments and suggested improvements to the Commander, III Corps and Fort Hood, ATTN: AFZF-GT-PO, Fort Hood, Texas 76544-5056.

**REQUIREMENTS IMPACTING ON UNIT COMMANDERS.** Requirements impacting on base cluster commanders (BCC) are listed in paragreph 2-14 of this regulation.

---

**TABLE OF CONTENTS**

CHAPTER	PAGE
Chapter 1 Introduction	1-1
Chapter 2 Planning for Combatting Terrorism (CBT/T)	2-1
Section I General	2-1
Section II Planning Committee Responsibilities	2-1
Section III Responsibilities	2-3
Chapter 3 CBT/T Procedures	3-1
Section I General	3-1
Section II Concept of Operation	3-2
Section III Threatcon Measures	3-5
Section IV Mission Essential and Vulnerable Areas (MEVA)	3-8
APPENDICES	
Appendix A References	A-1
Appendix B Combatting Terrorism Areas of Expertise	B-1
Appendix C Combatting Terrorism Planning Committees	C-1

**FOR OFFICIAL USE ONLY**



## CHAPTER 1

## INTRODUCTION

1-1. **PURPOSE.** This regulation establishes a document for Fort Hood that consolidates Combatting Terrorism (CBT/T) responsibilities and actions that must be accomplished by III Corps and Fort Hood elements to develop and maintain a unified, effective program. The program includes antiterrorism (defensive) and counterterrorism (offensive) measures and CBT/T planning. This regulation supersedes FH Reg 190-10 (Terrorism Counteraction (TC) Planning).

1-2. **REFERENCES.** References used in this regulation are listed in appendix A.

1-3. **EXPLANATION OF ABBREVIATIONS AND TERMS.** Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. **APPLICABILITY.** This regulation applies to the Fort Hood Installation and tenant organizations located on Fort Hood.

1-5. **GENERAL.** A variety of requirements and responsibilities relating to CBT/T exist for III Corps and Fort Hood. To be sure of a unified effort and to effectively administer CBT/T at Fort Hood, a single program to coordinate and monitor these actions is necessary. The Fort Hood CBT/T Program consolidates the requirements that encompass a viable program for CBT/T. The program establishes a plan for the protection of Fort Hood using the base cluster (BC) concept, FM 90-14 (Rear Battle) as a guide. (See chapter 3).

1-6. **RESPONSIBILITIES.** The overall proponent for CBT/T is the ACofS G3/Plans, Training, and Mobilization (PTM). The planning councils (see chapter 2) provide recommendations/approval on every aspect of CBT/T at Fort Hood and make sure the Commanding General (CG) is informed on CBT/T matters. Although the G3 has overall CBT/T responsibility, other command and staff elements have responsibilities in support of the program (appendix B). Additionally, the standards delineated in the program are minimum requirements that must be met. Some of the requirements necessitate additional planning by the units or other organizations for implementation. The G3 will task remaining units at Fort Hood to assume CBT/T responsibilities of deployed Fort Hood units when necessary.

1-7. **CLASSIFICATION GUIDANCE.** (Reference: CINCFOR Fort McPherson, Georgia, Message 171710ZJan91)

a. The fact that the command/installation has implemented terrorist threat condition (THREATCON) security measures is unclassified.

b. The fact that command/installation has implemented a specific THREATCON level is unclassified, **For Official Use Only (FOUO)**. Public release of specific THREATCON level is not authorized.

c. Specific measures implemented or excluded are confidential. However, acknowledgment of high visibility measures, e.g. additional gate guards, inspection of vehicles, etc, is authorized.

## CHAPTER 2

**PLANNING FOR CBT/T****SECTION I - GENERAL**

2-1. **CBT/T PLANNING.** CBT/T planning is done by the working group (WG) and senior council (SC). These councils are designed to identify, plan, and coordinate III Corps and Fort Hood staff actions necessary to promote and support CBT/T at Fort Hood. The membership of the WG and SC is established in appendix C.

2-2. **ACTION PRIORITIES.** Fort Hood has limited assets to be used for CBT/T and therefore needs a pro-active system to identify action priorities to reduce installation vulnerability to terrorist acts. These actions include:

- a. Identifying Mission Essential/Vulnerable Areas (MEVAs) (appendix D).
- b. Establishing military and civilian training objectives (appendix E).
- c. CBT/T Plan (chapter 3).

**SECTION II - PLANNING COMMITTEE RESPONSIBILITIES**

2-3. **PLANNING COMMITTEE.** The WG and SC are designed to provide a broad base of expertise for threat analysis and antiterrorist recommendations. They are strictly pro-active groups. Their responsibilities are limited to preparations to prevent or reduce the probability of terrorist incidents.

a. The WG is the primary pro-active group for CBT/T at Fort Hood. It serves as the commander's staff advisory group on the distribution of available resources to achieve optimum use to prepare for a possible terrorist incident.

b. The standard WG membership will meet quarterly to review new requirements and the status of ongoing actions assigned to a staff proponent. The WG can also be called into a special session if the need arises.

c. Additional members (appendix C) need to attend based on current issues in their area of expertise. Attendance can originate from either the standard WG or from the staff element itself. Additional members are informed of WG meetings, they then determine their need to attend, unless already required.

d. The WG has overall staff responsibility for recommendations concerning aspects of CBT/T at Fort Hood. In addition it:

- (1) Identifies installation vulnerabilities to a terrorist threat.
- (2) Centralizes efforts to harden targets and eliminate weaknesses.
- (3) Reviews, analyzes, and reports (with applicable recommendations) to the SC on the results of CBT/T exercises at Fort Hood.
- (4) Recognizes needs for additional installation contingency plans and recommends a proponent for each.
- (5) Provides changes to update operation plan (OPLAN) READY GO to ATTN: AFZF-PTM-PZ.
- (6) Oversees United States Forces Command (FORSCOM) Security Enhancement Plan (FSEP) (appendix F) implementation at Fort Hood.

- (7) Develops, maintains, and updates the Fort Hood CBT/T Program for FSEP implementation and other requirements related to CBT/T.
- (8) Recommends priorities for actions needed to support installation projects.
- (9) Considers the impact of possible CBT/T projects/programs and balances the possibilities within resource constraints to obtain optimum effect.
- (10) Recommends the allocation of available resources and substantiates the recommendations for cost, time, and expected impact.
- (11) Oversees training aspects relating to terrorism or CBT/T.
- (12) Determines the CBT/T status at Fort Hood.
- (13) Develops recommendations on CBT/T and related activities for submission to the Chief of Staff (CofS) and SC.
- (14) Combines crime prevention/physical security data with terrorist threat intelligence to provide the installation commander with accurate vulnerability assessments.
- (15) Continually updates the terrorist threat assessment and submits it to the proper headquarters and agencies as required.
- (16) Submits the minutes from WG meetings to the CofS for his information, and provides a copy to each WG member.

2-4. **SC RESPONSIBILITIES.** The SC is chaired by the CofS and serves as the commander's decision-making group. It keeps the commander updated on CBT/T at Fort Hood, and is the approval authority for recommended solutions, priorities, and resource allocation. The SC meets as required. It also:

- a. Reviews/makes decisions concerning WG recommendations.
- b. Informs the CG on CBT/T matters.
- c. Refers matters of concern to the WG for study and recommendations.
- d. Provides the CG with the status of installation CBT/T, and a summary of finances (including expenditures and unfinanced requirements).
- e. Prioritizes problems and recommendations.
- f. Responds to items in which the CG has expressed an interest.
- g. Submits the minutes from SC meetings to the CofS for approval.

2-5. **FUNCTIONAL SUBCOMMITTEE.** When the need arises, a functional subcommittee is formed to address a certain aspect of CBT/T problems or recommendations. The chairman and composition of the subcommittee is determined by project subject, purpose, and scope. Subcommittees perform the necessary actions to fully discharge the responsibility levied by the SC or WG.

**SECTION III - RESPONSIBILITIES**

2-6. **STAFF ACTIVITIES.** Staff activities remain responsible for their own functions associated with CBT/T (such as: engineering, intelligence, law enforcement, training, resource management, etc.). They perform these actions in accordance with (IAW) normal staff procedures, and must plan ahead and be prepared to take actions in their functional areas in the event of a terrorist incident. Most of these actions are part of standard operations, but may require a special adaptation for dealing with terrorist activities. Each staff representative informs the WG on CBT/T and related matters within the particular staff element. Each staff section prepares and coordinates budget requests dealing with CBT/T, with the WG and SC prior to commitment.

2-7. **G3 OPERATIONS/PTM.** G3/PTM has overall staff responsibility for CBT/T. G3/PTM:

- a. Convenes and conducts WG and SC meetings.
- b. Monitors the program of terrorist threat briefings, debriefings, and assessments for personnel going on leave, temporary duty (TDY), permanent change of station (PCS), or deploying to terrorist threat areas.
- c. Prepares installation operations plans and orders containing a terrorist threat assessment, instructions for defensive measures (if any), and reporting procedures IAW AR 525-13 (The Army Terrorism Counteraction (Combatting Terrorism) Program).
- d. Writes and maintains an antiterrorism plan for implementation of terrorist threat conditions and related requirements.

2-8. **G2 COUNTERINTELLIGENCE (CI)/DIRECTORATE OF SECURITY (DSEC).** G2 CI/DSEC maintains and provides terrorist threat information as permitted by Army policy. G2/DSEC also:

- a. Coordinates with the 504th Military Intelligence (MI) Brigade and the 902d MI Group Fort Hood Resident Office for current terrorism related intelligence support.
- b. Coordinates with the Provost Marshal Office (PMO) Physical Security in the identification and prioritization of probable terrorist targets to include high risk personnel, mission essential vulnerable areas and soft target facilities.
- c. Supports the requirement for inclusion of terrorist threat information in Subversion and Espionage Directed Against the Army (SAEDA) training through appropriate staff guidance and command inspections.
- d. Prepares and presents terrorist threat briefings to high risk personnel and their families.

2-9. **PROVOST MARSHAL (PM).** The PM develops/maintains physical security plans, surveys, and inspections. The PM also:

- a. Sees to the implementation of physical security preventive measures.
- b. Maintains a priority list of MEVAs.
- c. Coordinates actions for possible controlled access to/egress from the installation.
- d. Provides site surveys of MEVAs to determine intrusion detection system/closed circuit television (IDS/CCTV) or other protection needs for CBT/T.

2-10. **UNITED STATES ARMY CRIMINAL INVESTIGATIONS COMMAND (USACIDC).** USACIDC provides:

- a. Vulnerability assessments for key personnel.
- b. Crime prevention surveys for selected activities to integrate into WG vulnerability assessments.
- c. Criminal information and intelligence related to CBT/T as permitted.
- d. Crime scene processing and evidence collection.
- e. Hostage negotiations.
- f. Witness, survivor, escapee, and released personnel interviews.

2-11. **DIRECTORATE OF ENGINEERING AND HOUSING (DEH).** The DEH maintains the status of installation CBT/T measures and/or projects. DEH also:

- a. Provides engineering design assistance on suggested CBT/T physical security measures, including plans/designs for access control points (ACPs).
- b. Coordinates engineering designs with PMO for physical security equipment needs.
- c. Maintains blueprints for government controlled facilities and residences.

2-12. **STAFF JUDGE ADVOCATE (SJA).** SJA provides applicable legal guidance to the WG and SC for compliance with pertinent laws and regulations.

2-13. **DIRECTORATE OF RESOURCE MANAGEMENT (DRM).** DRM maintains status of force protection funds. The DRM also:

- a. Prepares III Corps security funding reports and presents them to the WG, SC, the Corps Commander and FORSCOM.
- b. Consolidates and coordinates force protection initiatives.
- c. Directs allocations of available funds as determined by the councils.
- d. Prepares CG's summary of finances (including expenditures and unfinanced requirements).

2-14. **BASE CLUSTER COMMANDERS (BCCs).** The BCC is responsible to:

- a. Secure and man the ACP's at THREATCON CHARLIE/DELTA.
- b. Implement THREATCON measures as directed.
- c. Develop base cluster (BC) OPLAN for implementing requirements of FH Reg 525-13.
- d. Prepare battle books IAW appendix J, this regulation. Identify contingency personnel to execute THREATCON measures/other requirements.
- e. Produce a diagram of each BC MEVA with appropriate guard instructions.
- f. Coordinate with other units in respective areas to enhance OPLANS.

- g. Maintain capability to rapidly respond to and implement THREATCON measures.
- h. Establish quick/reliable communication to BC and Corps Operation Center (COC).
- i. Be prepared to implement OPLAN READY GO/or the access control plan.
- j. Be prepared to draw ammo from ammunition supply point (ASP) and move it to ammunition holding area (AHA), or unit arms rooms IAW FH Pam 700-15 (Fort Hood Ammunition Handbook).
- k. At THREATCON CHARLIE, units within a BC come under the operational control (OPCON) of the BCC.
- l. Identify key operational personnel/maintain roster.
- m. Prepare telephonic request for ACP's/other appropriate locations.

Refer to Table 3-1, this regulation for BC requirements for THREATCON level.

CHAPTER 3  
CBT/T PROCEDURES

**SECTION I - GENERAL**

3-1. The CBT/T plan provides the ability, on short notice, to control access to Fort Hood, to secure identified MEVAs, and to implement the specified measures of the THREATCONs.

3-2. CBT/T consists of actions taken to reduce the vulnerability to a terrorist act (antiterrorism) and measures taken to prevent, deter and respond to a terrorist incident (counterterrorism). The manpower and equipment to conduct these operations require extensive major subordinate command(MSC) involvement.

3-3. This plan is modeled after the rear operations concept of base defense in FM 90-14. In order to maintain the ability to sustain access control, simultaneously securing and monitoring MEVAs, and/or to implement the specified measures under the THREATCONs, Fort Hood's installation areas have been divided into specific BCs for the MSCs (see appendix I).

Each BCC is responsible for securing and manning the ACP's at THREATCON CHARLIE, securing and monitoring the MEVAs, and enforcing measures under the designated THREATCONs, as directed. The PMO and DEH are responsible for planning and designing ACP's. Each BCC is responsible for the planning, preparation, supervision, and execution of plans for the protection of personnel, equipment, facilities, and resources within their area. Each BCC will develop an OPLAN to meet the requirements of this regulation and forward a copy to ACofS, G3, ATTN: AFZF-GT-PO. Battle books will also be prepared IAW appendix J, this regulation. A diagram of each MEVA and the activity responsible for manning it will be forwarded to III Corps with the BCs' plan. Each installation or tenant activity is subject to the command and control of the BCC where the activity is located upon implementation of this program. Close coordination between BCC's and units within their BCs must be accomplished to be sure of a workable plan. Command and control for the BC concept is through the COC/Emergency Operations Center (EOC) network.

3-4. **CANTONMENT AREAS AND ACPs.** The access control plan (see appendix H) identifies the ACPs for each of Fort Hood's three cantonment areas (Main, West, and North). Depending upon the current assessment, various control points may be completely closed rather than manned, but plans must be made to control access/egress at each of the points within a BC. Besides the ACPs, patrols may be required to help secure the installation perimeter if a potential vulnerability is identified. A specific gate and/or high priority screening lanes will be identified for entry of designated key personnel, emergency vehicles and wide/oversize loads.

**3-5. MEVA AND PERSONNEL.**

a. Facilities and personnel which have been designated as mission essential at Fort Hood are listed in appendix D, this regulation. Also included are charts depicting their vulnerability and the regulatory requirements for their protection. The regulatory requirements must be implemented. The MEVAs within a unit's perimeter must be secured and monitored as directed. MEVA priorities may change depending on the current threat.

b. Access to the security of the airfields (Robert Gray Army Airfield (RGAAF) and Hood Army Airfield (HAAF) and upgrades thereto are the responsibility of the respective airfield commander in coordination with designated BC's.

c. The military police (MP) station and the alarm monitor station are the responsibility of the PM.

3-6. **THREATCONs.** Section IV, this chapter, explains the system of terrorist THREATCONs from AR 525-13, appendix C. In addition to defining the THREATCONs and listing the specified measures required under each, the responsible office for overseeing the overall implementation of each security measure is identified. Units must be capable of rapidly responding to initiate the measures within their area.

3-7. **Threat Management Force (TMF).** The TMF is not to be confused with the WG, SC or the Crisis Management Team (CMT). This unit is a tactical action force that actually plans and executes the response to terrorist disruptions on the installation. The TMF should be of sufficient size to manage the disruption and will usually involve a command element, security element, negotiation team, special reaction team (SRT) and logistical element. The PM is the TMF Commander. OPLAN READY GO shows the responsibilities of the TMF.

3-8. **Communications.** For the CMT to effectively coordinate the diverse requirements, establishing and maintaining communications is vital. Deployed elements must have dependable and regular contact with the BC EOC and, in turn, the BC EOC's must have the same with the COC. Command, control, and communications will depend on the use of quickly employable assets using the garrison telephone system, FM communications, and messengers (See appendix L).

## **SECTION II - CONCEPT OF OPERATION**

3-9. **Normal Operations.** Under normal operations the procedures outlined in Section III of this chapter will be met by every facility owner/custodian. Installation and tenant units/activities within a BC will coordinate with the BCC for integration of the base defense plan in support of the BC. In the event of a terrorist incident while at normal operations or at any of the THREATCON levels, OPLAN READY GO will be implemented. The access control plan can be implemented as directed. The CG may declare THREATCON DELTA for Fort Hood or any THREATCON when he deems it necessary under the provisions of AR 525-13. At this time BCCs would begin to implement those tasks indicated in Section IV this chapter and the measures required at THREATCON DELTA (Section III this chapter).

3-10. **THREATCON ALPHA.** At THREATCON ALPHA the measures set forth under THREATCON ALPHA (Section III this chapter) will be implemented. Select members of the CMT (see OPLAN READY GO paragraph 3b (2) (a)) will be called in to determine specific actions to be taken. Security elements of the TMF are identified and under the operational control of the PM.

3-11. **THREATCON BRAVO.** At THREATCON BRAVO the measures required under THREATCON BRAVO (Section III this chapter) will be implemented. In addition to these requirements each BC will be prepared to draw the ammunition required for its security forces from the ASP and place it in the AHA, or unit arms room (IAW AR 190-14). Ammunition is defined as ammo for individual weapons, (i.e., 9mm, 38 cal., 45 cal., M16). Crew serve weapons, pyrotechnics, and explosives are not authorized. Issue and upload of ammunition will be on order. CMT determines additional specific measures as necessary.

3-12. **THREATCON CHARLIE.** At THREATCON CHARLIE the BC will secure the MEVAs within his BC IAW the guidelines in the Fort Hood Combatting Terrorism Program (FHCTP). The tasks in Section IV this chapter will be accomplished as well as the requirements under THREATCON CHARLIE (Section III this chapter). Ammunition will be issued to security forces. BC EOCs will be activated, the TMF will be on 30 minute standby, and communications will be established with both the guard force and the COC. Installation and tenant units/activities within a BC will be under the OPCON of the BCC. The Corps' EOC will be fully staffed. In the event of a terrorist incident while at THREATCON CHARLIE the TMF will respond. Access control will be implemented as directed by the CMT.

3-13. **THREATCON DELTA.** At THREATCON DELTA previous tasks and measures will be continued as well as those required by Sections III and IV, this chapter, for THREATCON DELTA. THREATCON DELTA is declared as a result of an incident occurring in the immediate area, or intelligence indicating that a terrorist action against a specific location or person is likely. Therefore previously stated reactions to an incident will be carried out. Terrorist incidents, suspected terrorist incidents, or credible terrorist threats will be reported immediately to the Corps EOC which will in turn follow reporting procedures in AR 525-13 and immediately report the incident to the local Federal Bureau of Investigation (FBI) office.

3-14. **KEY OPERATIONAL PERSONNEL.**

a. Fort Hood activities need to identify their key operational personnel, who are critical to the execution of each THREATCON level. These personnel are those required for Base Operating Information System (BASEOPS), life support activities, emergency services and contingency planning staffs.

b. The contingency planning staffs review the required actions in their battle books to support the declared THREATCON level. Contingency personnel are then identified to execute these actions.

c. Civilian and military personnel tours of duty may be changed to reduce the traffic congestion at the ACPS. The Directorate of Civilian Personnel (DCP) must coordinate with PMO for road closure information to allow proper notification of labor unions.

d. THREATCONS CHARLIE or DELTA may be implemented without any early warning. On order, the Public Affairs Office (PAO) will make a public announcement over local radio stations to alert personnel of increased security measures on Fort Hood and that only mission essential personnel are to come to work. Nonessential personnel will be notified by their chain of command/employer when to report for duty or work.

**TABLE 3-1 CONCEPT  
BC REQUIREMENTS BY THREATCON LEVEL**

BC Requirements by THREATCON Level

<u>THREATCON</u>	<u>Installation Actions</u>	<u>BC Requirements</u>
Normal	Day to Day Operations	Prepare Battle Books Coord btwn inst/tenant units/activities & the BCC
ALPHA	Access Control Plan READY GO o/o THREATCON Measures 1-9 Begin closing roads (App H, Sec II)	Review Battle Books Access Control Plan READY GO o/o THREATCON Measures 1-8 Report measure status to COC
BRAVO	THREATCON Measures 10-29	Prepare request for Ammo to AHA /Arms Room (draw ammo o/o)  THREATCON Measures 9-29 Prepare request for special security equip. Report measures status to COC
CHARLIE	Corps EOC Staffed CMT assembled TMF - PM CDR Access Control Plan  THREATCON Measures 30-39 Reduce access points (App H, Sec II)	BC EOC staffed Issue Ammo Execute Access Control Plan Guard MEVA 1 Conduct patrols READY GO o/o units to 30 Min Standby THREATCON Measures 30-39 Report incident and measures status to COC
DELTA	Report incident THREATCON Measures 40-50	Report incident to COC THREATCON Measures 40-50

**SECTION III - THREATCON MEASURES**

3-15. The Joint Chiefs of Staff (JCS) approved a system of THREATCONs which became effective 1 April 1986. This standardized the terrorist alert system throughout the Department of Defense (DOD). The security measures under each THREATCON are now specified, not recommended as under the old system. If a command decides not to implement specific measures under a declared THREATCON, then the measures not taken and the rationale must be reported to the next higher headquarters, up to the JCS. The declaration of these THREATCONs and implementation of the measures may be decreed by a US command agency or by the Commander III Corps and Fort Hood following receipt of intelligence through official sources or following an anonymous threat.

3-16. The following THREATCON information is extracted from AR 525-13. Added to each of the specified measures is the responsible party for overseeing the proper implementation of the measure. This does not relieve anyone else of their responsibility to plan for and implement actions to accomplish the measures within their area of jurisdiction. Where more than one element is listed, the order of responsibility is shown. BC's must report their THREATCON measures implementation status to the COC every six hours until directed measures are implemented.

3-17. NORMAL: Day to day operations.

3-18. THREATCON ALPHA. This condition applies when there is a general threat of possible terrorist activity against installations, facilities and personnel, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain selected measures from higher THREATCONs resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

a. Measure 1. At regular intervals, remind personnel, including family members, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; to be alert for unidentified vehicles on, or in the vicinity of U.S. installations, units, or facilities; and to be alert for abandoned parcels or suitcases or any unusual activity. (\*PAO/UNITS\*)

b. Measure 2. Keep available the duty officer or other appointed personnel who have access to plans for evacuating buildings, or sealing off buildings/areas in use or where an explosion or attack has occurred. Keep key personnel who may be needed to implement security plans on call. (\*G3,BC\*)

c. Measure 3. Secure buildings, rooms, and storage areas not in regular use. (\*UNITS/OWNERS\*)

d. Measure 4. Increase security spot checks of vehicles and persons entering installations and nonclassified areas under the jurisdiction of the US command or agency. (\*PMO\*)

e. Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic. (\*PMO\*)

f. Measure 6. As a deterrent, apply one of the following measures from THREATCON BRAVO individually and randomly:

(1) Secure and regularly inspect buildings, rooms, and storage areas not in regular use. (Measure 14) (\*UNITS-OWNERS\*)

(2) At the beginning and end of each workday and at regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages. (Measure 15) (\*UNITS-OWNERS\*)

(3) Check deliveries to messes, clubs, and so forth. Advise family members to check home deliveries. (Measure 17) (\*Directorate of Personnel and Community Activities (DPCA), OWNER, PAO\*)

(4) As resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and build confidence among staff and family members. (Measure 18) (\*PMO, OWNER\*)

g. Measure 7. Review plans, orders, personnel details, and logistic requirements related to the introduction of a higher THREATCON. (\*G3, DSEC, BC\*)

h. Measure 8. As appropriate, review and implement security measures for high-risk personnel (for example, direct use of inconspicuous body armor). (\*PMO\*)

i. Measure 9. Spare for command use.

3-19. THREATCON BRAVO. This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable or being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

a. Measure 10. Repeat measure 1 and warn personnel of any other form of attack terrorists may use. (\*PAO/UNITS\*)

b. Measure 11. Keep on call personnel involved in implementing antiterrorist contingency plans. (\*G3,BC\*)

c. Measure 12. Check plans for implementation of the measures contained in the next higher THREATCON. (\*G3, DSEC, BC\*)

d. Measure 13. Where possible, cars and such objects as crates and trash containers are to be moved at least 25 meters from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking. (\*UNITS\*)

e. Measure 14. Secure and regularly inspect buildings, rooms, and storage areas not in regular use. (\*UNITS-OWNERS\*)

f. Measure 15. At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages. (\*UNITS-OWNERS\*)

g. Measure 16. Increase examination of mail for letter or parcel bombs. (\*Directorate of Information Management (DOIM)\*)

h. Measure 17. Check deliveries to messes, clubs, and so forth. Advise family members to check home deliveries. (\*DPCA, OWNER, PAO\*)

i. Measure 18. As resources will allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and family members. (\*PMO, OWNERS\*)

j. Measure 19. Make staff and family members aware of the general situation in order to stop rumors and prevent unnecessary alarm. (\*PAO/UNITS\*)

k. Measure 20. At an early stage, inform members of local security committees of any action being taken and why. (\*DSEC, G3, PMO\*)

l. Measure 21. Physically inspect visitors to the unit and a percentage of their suitcases, parcels, and other containers. (\*UNITS\*)

- m. Measure 22. Wherever possible, operate random patrols to check vehicles, people, and buildings. (\*PMO\*)
- n. Measure 23. Protect off-base military personnel and transport IAW prepared plans. Remind drivers to lock parked vehicles and institute a positive system of checking before entering and driving a car. (\*UNITS, PAO\*)
- o. Measure 24. As appropriate, implement additional security measures for high-risk personnel. (\*PMO\*)
- p. Measure 25. Brief augmentation guard force on use of deadly force. (\*BC\*)
- q. Measures 26-29. Spares for command use.

3-20. THREATCON CHARLIE. This condition applies when an incident occurs or when intelligence is received indicating that some form of terrorist action against installations, facilities and personnel is imminent. Implementation of this measure for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

- a. Measure 30. Continue THREATCON BRAVO measures or introduce those outstanding.
- b. Measure 31. Keep personnel responsible for implementing antiterrorist plans available at their places of duty. (\*G3,BC, DSEC\*)
- c. Measure 32. Limit access points to absolute minimum. (\*BC\*)
- d. Measure 33. Strictly enforce entry control and search a percentage of vehicles. (\*BC\*)
- e. Measure 34. Enforce centralized parking of vehicles away from sensitive buildings. (\*BC, PMO, Units-OWNERS\*)
- f. Measure 35. Issue weapons to guards. (Local orders should include specific orders on issue of ammunition). (\*BC\*)
- g. Measure 36. Introduce increased patrolling of the installation. (\*BC\*)
- h. Measure 37. Protect designated vulnerable points giving special attention to those outside military establishments. (\*BC, PMO, SJA\*)
- i. Measure 38. Erect barriers and obstacles to control traffic flow. (\*BC, PMO, DEH\*)
- j. Measure 39. Spare for command use.

3-21. THREATCON DELTA. This condition applies in the immediate area where a terrorist attack has occurred or intelligence has been received that terrorist action against a specific location, facility or person is likely. This THREATCON is normally issued as a localized warning.

- a. Measure 40. Continue or introduce measures listed for THREATCONs BRAVO and CHARLIE.
- b. Measure 41. Augment guards as necessary. (\*BC, PMO, UNITS\*)
- c. Measure 42. Identify vehicles already on the installation within operational or mission support areas. (\*BC, PMO, UNITS-OWNERS\*)

- d. Measure 43. Search vehicles and their contents entering the complex or installation. (\*BC, PMO, SJA\*)
- e. Measure 44. Control installation access, and implement positive identification of personnel. (\*BC, PMO, SJA\*)
- f. Measure 45. Search baggage such as suitcases, packages, and briefcases, brought into the complex or installation. (\*BC, PMO, SJA\*)
- g. Measure 46. Take measures to control access to areas under the jurisdiction of the U.S. command or agency concerned. (\*BC, PMO, SJA\*)
- h. Measure 47. Make frequent checks of the exterior of buildings and parking areas. (\*BC, PMO, UNITS-OWNERS\*)
- i. Measure 48. Minimize administrative journeys and visits. (\*UNITS\*)
- j. Measure 49. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attack. (\*SJA, PMO\*)
- k. Measure 50. Spare for command use

#### SECTION IV - MISSION ESSENTIAL AND VULNERABLE AREAS (MEVA)

3-22. Mission essential refers to facilities/activities on the installation which, by virtue of their function, are essential to successful accomplishment of III Corps' and Fort Hood's mission. As such, actions must be taken to protect them from destruction and disruption. In addition to being able to control access to the cantonment areas, we must be able to secure and monitor these mission essential areas as necessary.

3-23. Vulnerable refers to areas nonessential to the installation's operational mission, but which, by nature of the activity, may be susceptible to theft, trespass, damage or other criminal activity.

3-24. The prioritization of the MEVAs is in appendix D.

3-25. The MEVAs and personnel; their vulnerability to bombing, sabotage, unauthorized entry, and hostage taking; and the regulatory requirements for their protection, are also in appendix D. THREATCON requirements are at Sections II, III, and IV this chapter.

#### 3-26. PRIORITY RANKING.

a. PRIORITY 1. Activities or facilities which if compromised, would virtually stop the installation's accomplishment of its assigned national security mission.

b. PRIORITY 2. Activities or facilities which if compromised, would seriously damage the installation's capability to accomplish its other assigned missions.

c. Other. These are other Fort Hood activities/facilities that are on the MEVA list. Activities or facilities which if compromised, would hamper the ability of the installation to perform its assigned mission. This includes facilities used to store material, which, if stolen, would have an adverse effect on public order and the security of the installation, or which would have a potential for use by terrorist or anarchist groups in attempting to overthrow the government of the U.S. by forcible means. This grouping also includes activities or facilities used for storage of material which has a pecuniary value, or which, if compromised, damaged, or destroyed would seriously affect morale or the welfare of the troops. Also included are areas that would be considered vulnerable, defined as: areas nonessential, but which may be susceptible to theft, trespass, damage or other criminal activity.

## 3-27. SECURITY RESPONSE REQUIREMENTS.

a. General response requirements - Guards will be armed at THREATCON CHARLIE or as directed by the CG III Corps and Fort Hood, and have live ammo on their person, but not in the weapon. Each guard force will consist of at least a two man team. The actual size will be determined by the responsible BCC. Each guard force will have communications with the BC's EOC. Upon arrival at Priority 1 MEVAs the guard force will provide the BC EOC with a situation report. The BC EOC will in turn report to the Corps EOC. Upon initial arrival at Priority 2 and other MEVAs the guard force will notify the BC EOC which will in turn notify the Corps EOC. After that reporting cycles will be determined by the BCCs, except that any unauthorized presence will be reported to the BC EOC, and in turn the Corps EOC, upon identification.

b. PRIORITY 1 Response Required - A continuous armed guard. BCCs will guard the Priority 1 MEVAs within their BC within one hour of notification from COC. Priority 1 MEVAs will be manned continuously. Each of the above listed general requirements apply, unless directed otherwise by the Corps EOC.

c. PRIORITY 2 Response Required - Frequent checks by an armed guard force. Frequent is defined as at least once every hour at varied intervals. Guards will be checking for signs of unauthorized presence. Each of the above listed general requirements apply, unless directed otherwise by the Corps EOC.

d. Other MEVAs will be checked periodically by an armed guard force for signs of unauthorized presence. Periodic is defined as at least every six hours at varied intervals. Each of the above listed general response requirements apply, unless otherwise directed by the Corps EOC.

e. Security guards will be given a use of force/rules of engagement briefing prior to being issued ammunition. The rules of engagement for the use of deadly force are specified in appendix K which is IAW AR 190-14 (Carrying of Firearms and Use of Force for Law Enforcement and Security Duties).

f. MEVAs will be evaluated to determine if further augmentation is required.

g. MEVA priorities are subject to change based on threat and vulnerability assessments.

FOR THE COMMANDER;



PAUL T. WEYRAUCH  
Brigadier General, GS  
Chief of Staff

STEPHEN J. BERTOCCHI  
LTC, SC  
DOIM

- 15 Appendices
- A. References
- B. Combatting Terrorism Areas of Expertise
- C. Combatting Terrorism Planning Committees
- D. Mission Essential/Vulnerable Areas (MEVAs)
- E. Combatting Terrorism Training Requirements
- F. Summary of FORSCOM Security Enhancement Plan
- G. Summary of OPLAN READY GO
- H. Access Control Plan
- I. Base Clusters/Maps

- J. Battle Book Guidance
- K. Deadly Force
- L. Base Cluster Signal Instructions
- M. Inspection Procedures
- N. Situation Dependent Questions to be Answered by Command  
Glossary

DISTRIBUTION:  
IAW FH Form 1853, C  
Plus: IM-AO (2)  
IM-ARL (1)  
IM-Pubs (100)

**APPENDIX A**

**REFERENCES**

- AR 190-13        The Army Physical Security Program
- AR 190-14        Carrying of Firearms and Use of Force for Law Enforcement and Security Duties
- AR 210-10        Installation Administration
- AR 381-12        Subversion and Espionage Directed Against U.S. Army
- AR 525-13        The Army Terrorism Counteraction (Combatting Terrorism) Program
- FM 90-14         Rear Battle
- FM 100-37        Terrorism Counteraction
- TC 19-16         Countering Terrorism on U.S. Army Installations
- DA Pam 190-52    Personal Security Precautions Against Acts of Terrorism
- FH Pam 700-15    Fort Hood Ammunition Handbook
- FORSCOM Security Enhancement Plan (FSEP)
- III Corps and Fort Hood Special Threat OPLAN, Short Title: READY GO
- Fort Hood Installation Physical Security Plan
- DAMO-ODZ msg DTG 281815Z Feb 89, SUBJECT: Terrorism Terminology
- The Security Engineering Manual (FOUO)

## APPENDIX B

## COMBATTING TERRORISM AREAS OF EXPERTISE

AREA	RESPONSIBLE STAFF AGENCY
Policy, Plans, and guidance	G3
Threat conditions (THREATCONs)	G3
Training	G3
Antiterrorism	G3
Intelligence	G2/DSEC
Engineering functions	DEH
Funding	DRM
Legal	SJA
Counterterrorism	PM
Physical/personal security	PM
Special Reaction Team (SRT)	PM
Public Affairs	PAO
Hostage Negotiations/Crime Scene Processing	USACIDC
Signal Instructions	ACSO

APPENDIX C

COMBATTING TERRORISM PLANNING COMMITTEES

WORKING GROUP (WG)

SENIOR COUNCIL (SC)

Standard Members

G3, Ops  
PTM  
G2/DSEC  
PMO  
SJA  
DEH  
DRM  
Corps BC's  
CID

CofS  
ACofS, G3  
G3, Ops  
PTM  
G2/DSEC  
PMO  
SJA  
DEH  
DRM  
Corps BC's

Additional Members:

ACofS, G1  
Adjutant General  
DPCA  
Chaplain  
ACofS, G2  
ACofS, G4  
ACofS, G5  
G3, Resource Mgmt  
G3, Soldier Ed Div  
Headquarters Command  
Installation Aviation Office  
Installation Airfields Commander  
COC  
Corps Signal  
DOIM/USAISC  
USACIDC  
DHS  
TEXCOM  
DPC  
DOL  
DRCS  
PAO  
DOC  
EOD  
DACH

**NOTE:** Other WG members may be required to attend based on specific issues/recommendations.

CRISIS MANAGEMENT TEAM (CMT)

CofS  
G3/G3 OPS  
G2/902nd  
PMO  
SJA  
G1  
G4  
PAO  
DEH  
DOIM  
CID  
Corps BCC's

**THREATCON CHANGE NOTIFICATION**

1. **SITUATION:** THREATCON messages must be disseminated as soon as practical.
2. **MISSION:** The COC disseminates THREATCON information when it receives a message directing the action and or upon direction of G3 or Commander.
3. **EXECUTION:** After advising G3, G3 OPS, G2 and PMO, make notifications listed below (Record initials of persons contacted).

(A) Obtain a copy of the message and reproduce in sufficient quantities to provide copies to every agency.

(B) **CLASSIFICATION GUIDANCE:** The fact that the THREATCON level has changed or that III Corps is at a specific THREATCON level is **CLASSIFIED FOUO**. Our THREATCON level may be stated on Unsecure telephones. The reason why a THREATCON level changes may be **CLASSIFIED** and the notification message should be reviewed for security guidance.

(C) State the following to the units and agencies notified.  
 'THIS IS THE III CORPS COMMAND OPERATIONS CENTER. AN IMMEDIATE MESSAGE PERTAINING TO THREATCON HAS ARRIVED HERE AT THE OPERATIONS CENTER (BUILDING 1001). THIS MESSAGE PERTAINS TO YOUR UNIT. PICK UP THIS MESSAGE AND DISSEMINATE THE INFORMATION AS SOON AS PRACTICAL. TELEPHONICALLY REPORT COMPLIANCE WITH THE MEASURES OUTLINED NLT 3 HOURS FROM RECEIPT OF THIS NOTIFICATION. PHONE 287-2520 OR 287-2506. (REPEAT NUMBERS)'

		TIME NOTIFIED	CONF #1	TIME COMPLETED
<input type="checkbox"/> G3	* 410/492	_____	<input type="checkbox"/> 1CD	*443
<input type="checkbox"/> G3 OPS	*411/634/9810	_____	<input type="checkbox"/> 6CB (AC)	*454
<input type="checkbox"/> G2	*409/ON CALL	_____	<input type="checkbox"/> 504 MI	*460
<input type="checkbox"/> DEH	*422/7-7131	_____	<input type="checkbox"/> 31 ADA	*597
<input type="checkbox"/> DCP	*287-7803/ON	_____	<input type="checkbox"/> 3 SIG	*455
	CALL	_____	<input type="checkbox"/> 89 MP	431
<input type="checkbox"/> DOIM	*287-3635/2101	_____	<input type="checkbox"/> 3 FIN	463
<input type="checkbox"/> SJA	*287-3421/ON	_____	<input type="checkbox"/> ATB	540
	CALL	_____	<input type="checkbox"/> 13 COSCOM	451
<input type="checkbox"/> CID	*287-2722/5039	_____		
<input type="checkbox"/> GCDR	*287-2205	_____		
<input type="checkbox"/> G1	*408	_____		
<input type="checkbox"/> G4	*416	_____		
<input type="checkbox"/> PAO	*7-7823	_____		
<input type="checkbox"/> FORS-		_____		
<input type="checkbox"/> COM	367-5222	_____		
<b>CONF #2</b>		<b>TIME COMPLETED</b>	<b>CONF #3</b>	
<input type="checkbox"/> RANGE CONTROL	412	_____	<input type="checkbox"/> NCOA	7-0222/AFTER HOURS 4038
<input type="checkbox"/> PMO	*432	_____	<input type="checkbox"/> 21 REPL	7-4549
<input type="checkbox"/> DACH	*481	_____	<input type="checkbox"/> NFH (DRC)	8-0115
<input type="checkbox"/> PHANTOM CMD	*437	_____	<input type="checkbox"/> NETT, JTF	8-1081
<input type="checkbox"/> TEXCOM	479	_____	<input type="checkbox"/> 7-7809	
<input type="checkbox"/> 3 PERS GROUP	550	_____	<input type="checkbox"/> 7-5943	
		<input type="checkbox"/> AVSCOM	<input type="checkbox"/> BELTON LAKE	7-0309
		<input type="checkbox"/> COMMISARY	<input type="checkbox"/> G3 XO	7-2203
<b>NON CONFERENCE</b>		<b>TIME NOTIFIED</b>	<input type="checkbox"/> SGS	7-7806
<input type="checkbox"/> 4ID (FWD)	7-5959/8703	_____	<input type="checkbox"/> GTE	532-2550
<input type="checkbox"/> 5ID (FWD)	8-5345/5383	_____		
<input type="checkbox"/> RGA AF	413	_____		
<input type="checkbox"/> HAA F	414	_____		
<input type="checkbox"/> DOL	424	_____		
<input type="checkbox"/> G5	417	_____		
<input type="checkbox"/> DRC	418	_____		
<input type="checkbox"/> DSEC	514	_____		

ACTION OFFICER  
 OPERATIONS SGT  
 JOURNAL NUMBER  
 ENCLOSURE NUMBER

\*CRISIS MANAGEMENT TEAM HAS PRIORITY OF NOTIFICATION  
**AFTER HOURS NOTIFY APPROPRIATE ON CALL REPRESENTATIVE**

TERRORIST INCIDENT NOTIFICATION

- 1. SITUATION: A potential terrorist incident has been reported to the COC. (bombing, shooting, assassination, hostages, etc.)
- 2. MISSION: The COC notifies III Corps staff members, MSC's and staff elements of the terrorist incident.
- 3. EXECUTION:
  - (A) Notify the G3 of his representative.
  - (B) Record initials of persons contacted and time of notification.
  - (C) Notify the crisis management team when directed by the G3. Have them report to the COC conference room Bldg 1001 as soon as possible.
  - (D) Notify agencies listed below.

THE COC HAS BEEN NOTIFIED OF: 'STATE THE FOLLOWING'  
 (type of incident) WHICH  
 OCCURRED AT: (location of incident & time of incident)

- (E) Complete an Emergency Response Report.
- (F) After hours notify appropriate on call representative.

	TIME NOTIFIED	CONF #1	TIME COMPLETED
- G3	* 410/492	___ 1CD	*443
___ G3 OPS	*411/634/9810	___ 6CB (AC)	*454
___ G2	*409/ON CALL	___ 504 MI	*460
___ DEH	*422/7-7131	___ 31 ADA	*597
___ DCP	*287-7803/ON	___ 3 SIG	*455
	CALL	___ 89 MP	431
___ DOIM	*287-3635/2101	___ 3 FIN	463
___ SJA	*287-3421/ON	___ ATB	540
	CALL	___ 13 COSCOM	451
___ CID	*287-2722/5039		
___ GCDR	*287-2205		
___ G1	*408		
___ G4	*416		
___ PAO	*7-7823		
___ FORS-			
___ COM	367-5222		

CONF #2	TIME COMPLETED	CONF #3	TIME COMPLETED
___ RANGE CONTROL	412	___ NCOA	7-0222/AFTER HOURS 4038
___ PMO	*432	___ 21 REPL	7-4549
___ DACH	*481	___ NFH (DRC)	8-0115
___ PHANTOM CMD	*437	___ NETT, JTF	8-1081
___ TEXCOM	479	___ 7-7809	
___ 3 PERS GROUP	550	___ 7-5943	
	___ AVSCOM	___ BELTON LAKE	7-0309
	___ COMMISARY	___ G3 XO	7-2203

NON CONFERENCE	TIME NOTIFIED		
___ 4ID (FWD)	7-5959/8703	___ *SGS	7-7806
___ 5ID (FWD)	8-5345/5383	___ GTE	532-2550
___ RGAAF	413		
___ HAAF	414		
___ DOL	424		
___ G5	417		
___ DRC	418		
___ DSEC	514		

- \_\_\_ ACTION OFFICER
- \_\_\_ OPERATIONS SGT
- \_\_\_ JOURNAL NUMBER
- \_\_\_ ENCLOSURE NUMBER

\*CRISIS MANAGEMENT TEAM HAS PRIORITY OF NOTIFICATION

**THREATCON MEASURES IMPLEMENTATION STATUS FOR COC.**

THREATCON Measures to be implemented:

<u>MSC</u>	<u>AREA</u>	<u>MEASURES IMPLEMENTED</u>	<u>MEASURES TO IMPLEMENT</u>
504th Time:	1 RMKS:		
31 ADA Time:	2 RMKS:		
1CD Time:	3 RMKS:		
13COSCOM Time:	4 RMKS:		
3SIG Time:	5 RMKS:		
HQ CMD Time:	6 RMKS:		
TBD Time:	7 RMKS:		
6CB (AC) Time:	8 RMKS:		
NFH Time:	9 RMKS:		

APPENDIX D  
MISSION ESSENTIAL/VULNERABLE AREAS (MEVAs)

## SECTION I - PRIORITIZATION AND RESPONSIBILITIES

MEVA priorities may change according to the current threat situation. Special instructions concerning MEVA guard requirements will be provided by Corps G3 in fragmentary order 9FARGO) format.

<u>MISSION ESSENTIAL/VULNERABLE AREAS</u>	<u>PRIORITY</u>	<u>RESP UNIT</u>
III Corps HQ Bldg 1001	1	HQ CMD
Main Electrical Power Station 100	1	HQ CMD
Weapons Warehouse Bldg 90031	1	504 MI
Bldgs 11 (Central) & 13 (DOIM)	1	HQ CMD
Alarms Monitor Station (Bldg 2204)	1	PMO
Arms Rooms	1	W/O Opnl JSSIDS
Airfields HAAF, RGAFF	1	6CB, 504 MI
Main Petroleum Oil and Lubricant (POL) Complex Clarke Road & US 190	1	31 ADA
Ammo Holding Area	1	1 CD
Ammo Supply Point	1	504 MI
Small Arms Repair, Bldg 88038	1	31 ADA
Sensitive Compartmented Information Facility (SCIF), Bldg 90088	1	504 MI
Arms Rooms	2	W/Opnl JSSIDS
Landing Zone Phantom	2	31 ADA
Natural Gas Meters & Valves (Main Trans Line)	2	1CD, 504 MI, 6 CB
Electrical Power Station (Bldgs 92040, 93043)	2	504 MI
Main Water Storage Facilities	2	3 SIG, 504 MI, 31 ADA
Primary Water Pumping Stations	2	3 SIG
POL Storage Tanks	2	1CD, 3 SIG, 504 MI, COSCOM
SCIFS, Bldgs 16001, 22012, 27002, 91002	2	1CD, 504 MI
OTHER HQ BLDGS (410, 28000, 91012)	2	1CD, 504 MI
Darnall Army Community Hospital (Bldg 36000)	2	COSCOM
Automatic Data Processing Activities Bldg 40001 (DOL Maintenance)	2	COSCOM

<u>MISSION ESSENTIAL/VULNERABLE AREAS</u>	<u>PRIORITY</u>	<u>RESP UNIT</u>
Regional Data Center (1901 South Clear Creek Rd)	2	COSCOM
Motor Pools	2	ALL
Approach Radar, Radio Transmitter Site	2	504 MI
Air Traffic Control	2	504 MI
Beacon Hill (PK125374)	2	504 MI
Gas Pipeline North Fort Hood	Other	3 SIG
Water Storage Facilities on Pipeline	Other	
Secondary Water Pumping Stations	Other	504 MI
Telephone Exchanges Bldgs 56303, 91001	Other	3 SIG, 504 MI
Railroad Overpass (Main Gate)	Other	
Flight Simulators, Bldgs 7019, 7050, 7051	Other	6 CB (AC)
Bulk Storage Facilities	Other	All
Dry Storage/Cold Storage, Bldg 4238/4612	Other	COSCOM
Transportation Motor Pool	Other	COSCOM
Nuclear Weapons Maint & Trng, Bldg 5000	Other	31 ADA
Petroleum, Oil, Lubricants Bulk Storage	Other	6CB, COSCOM
Railhead/Switching Yard	Other	COSCOM
Finance Officer	Other	1 CD, COSCOM
Medical Warehouse, Bldg 4264	Other	COSCOM
Blood Bank/4448, 4449	Other	3 SIG
North Fort Hood (NFH) Water Tanks and Pumps	Other	3 SIG
Medical Storage	Other	504 MI
Sewage Treatment Trans Line (On Post)	Other	1 CD, 504 MI, COSCOM
Electric Power Substation, NFH	Other	3 SIG
Emergency High Frequency (EHF) Station (MARS) Bldgs 90001, 90002	Other	504 MI
Soldiers/Units		
Barracks	Other	All
Dining Facilities	Other	All
Clubs: NCO, Officer	Other	1 CD, 504 MI, 6 CB

**30 May1991**

**FH Reg 525-13**

MISSION ESSENTIAL/VULNERABLE AREAS

PRIORITY

RESP UNIT

Troop Medical and Dental Clinics	Other	1 CD, 6 CB, 504 MI, COSCOM
Banks/Credit Unions (Bldgs 137, 50005, 322)	Other	31 ADA, PMO
Battle Simulation Center Complex	Other	3 SIG
Military Police Station, Bldg 23020	Other	PMO
Families/Dependents/Retirees		
Post Exchanges/Bldgs 50004, 136	Other	31 ADA, PMO
Commissary Main, Bldg 50001	Other	31 ADA, PMO
Commissary Annex, Bldg 512	Other	PMO
Schools	Other	PMO, 31 ADA
Child Development Centers	Other	3 SIG, PMO, 31 ADA
Housing Areas	Other	504 MI, 31 ADA, PMO
Shoppettes	Other	1 CD, 504 MI

**SECTION II - VULNERABILITIES AND REQUIREMENTS**

---

FACILITY	*VULNERABILITY	REGULATORY REQUIREMENTS
----------	----------------	-------------------------

---

Bomb Sabo UnEn Hstg

Command and Control

III Corps, 1CD, and Test and Experimental Command (TEXCOM) Hqs Bldgs

Harden offices of high risk personnel (HRP) Metal 120 degree peephole. Door frame resistant to forced entry. Heavy-duty hinges on entrance doors w/nonremovable hinge pins and metal door pins. Windows will have adequate locking devices and shades or mylar. Windows within arms reach of entrance door's locks will be protected with bars or grills. Flush type entrance doors will have mortised, pin/tumbler lock with guarded latch and auxiliary, keyless, vertical deadbolt. Intrusion Detection System (IDS). Body alarms will be available. An interior room will be a safe haven and have means of communication with PMO. Utility shut-off valves will be locked. A fire protection system is required security lighting, access control procedures, vehicle parking design, CCTV protective standoff distances, exterior barriers.

FACILITY	*VULNERABILITY			REGULATORY REQUIREMENTS
	Bomb	Sabo	UnEn	Hstg
<u>Ammo, Wpns, Explosives</u>				
Ammo Supply Point (Cat I & II bunkers)	X		X	Security lightning, protective barrier, IDS
Ammo Holding Area			X	Protective barriers, lighting
Nuclear Wpn Maint & Trng (Bldg 5000)	X			Protective barriers, lighting
Arms Room	X			IDS, security lighting outside. Structural standards
Wpn Warehouse (Bldg 90031)	X			IDS, arms room structural standards
Small Arms Repair (Bldg 88038)	X			IDS, security lighting outside. Structural standards
<u>Key Communications</u>				
Main Communications Center Center (COMCEN) Bldg 13	X	X	X	Security lighting, access control procedures
Telephone Exchange (Bldgs 56303, 91001)	X	X		Locked buildings
ADP Activities (Bldgs 13, 36000, 40001)	X	X		Protective barriers, lighting, access control procedures
<u>Classified Storage</u>				
SCIFs (Bldgs 27002, 26001 90088, 91002, 13, 1001)	X	X	X	Protective barriers, lighting, access control procedures
Communications Security (COMSEC) Activities		X		Protective barriers, security lighting
EHF Station (MARS) (Bldgs 90001, 90002)	X	X	X	Security lighting, access control procedures, protective barriers
<u>Air Deployment</u>				
Airfields, RGAAF/HAAF	X	X	X	Protective barriers, security lighting, roving guards
Army Radar Approach Control (RGAAF)		X		Protective barriers, security lighting
Radio Transmitter Site	X	X		Protective barriers, security lighting

FACILITY	*VULNERABILITY				REGULATORY REQUIREMENTS
	Bomb	Sabo	UnEn	Hstg	
<u>Rail Deployment</u>					
Railhead/Switching Yard	X	X			None
Railroad Overpass (Main Gate)	X				None
<u>Major Utilities</u>					
Electric Power Stations/ Substations	X	X			None
Primary Pumping Stations/ Secondary		X	X		None
Main Water Tank	X	X			None
Pump Houses & Tanks on Pipeline (off post)	X	X			None
NFH Water Tanks & Pumps	X	X			None
Sewage Treatment Trans Line (on post)	X	X			None
<u>POL Operations</u>					
Main POL Storage Tank/ POL Bulk Storage	X	X	X		Security lighting, perimeter fence
Natural Gas Meters & Valves (main trans line)	X	X			None
Gas Pipeline (NFH)	X	X			None
<u>Security Monitoring</u>					
Military Police, Bldg 23020	X	X	X		None
Alarm Monitor Station Bldg 2204	X	X			Protective barriers, security lighting, duress alarm.
<u>Medical</u>					
Darnall Army Community Hospital, Bldg 36000	X	X	X	X	IDS (pharmacies), security lighting
Medical Warehouse, Bldg 4264	X				Protective barriers, security lighting
Medical Storage	X				Protective barriers, security lighting

FACILITY	*VULNERABILITY				REGULATORY REQUIREMENTS
	Bomb	Sabo	UnEn	Hstg	

Ground Transportation

Motor Pools	X	X	X		Protective barriers, security lighting
DOL Maintenance, Bldg 40001	X	X			Protective barriers, security lighting
TMP	X		X		Protective barriers, security lighting

Bulk Storage

Bulk Storage Facilities		X			Perimeter fence, security lighting
Dry Storage/Cold Storage		X			None

High Volume Money Handling

Finance Offices	X				None
Banks/Credit Unions (Bldg 137, 50005, 322, 90013)		X			None

Key Sensitive Training

Battle Simulation Center Complex	X				Protective barriers, security lighting
Flight Simulators (Bldg 7019, 7050, 7051)	X				Secure structure

**SECTION III - MISSION ESSENTIAL/VULNERABLE PERSONNEL VULNERABILITIES AND REQUIREMENTS**

PERSONNEL	*VULNERABILITY				REGULATORY REQUIREMENTS
	Bomb	Sabo	UnEn	Hstg	

High Risk Personnel (HRP)

HRP specified by CG	X			X	Duress system, security lighting, harden residence, body alarms
---------------------	---	--	--	---	---

Soldiers/Units

Barracks	X		X		None
Dining Facilities	X		X		None
Troop Clinics: Medical/Dental	X		X		None
Clubs: NCO, Officer	X		X	X	None

PERSONNEL	*VULNERABILITY				REGULATORY REQUIREMENTS
	Bomb	Sabo	UnEn	Hstg	

Families/Dependents/Retired

Housing Areas	X		X	X	None
Commissary (Bldg 50001, 512)	X				Protective lighting
Post Exchanges	X				Protective lighting
Shoppettes	X				Protective lighting
Schools	X		X	X	None
Child Development Centers	X			X	None

**NOTE:** Selected areas marked 'none' require access controls IAW AR 190-13 when declared a restricted area.

\*VULNERABILITIES:

- Bomb - Bombing
- Sabo - Sabotage
- UnEn - Unauthorized Entry
- Hstg - Hostage Taking

## APPENDIX E

**COMBATTING TERRORISM TRAINING REQUIREMENTS****SECTION I - BASIC TRAINING LEVELS**

## E-1. GENERAL

a. The following listings show what should be considered as the basic training levels needed to implement and sustain the CBT/T Program.

b. Quota requests should be submitted through the normal training channels. Attaining and maintaining the proficiency gained through this training is the long-term goal. Depending on the availability of quotas, courses similar to those shown can be used to obtain the required training. If prioritization of training becomes necessary, G3 Soldier Education Division will request a determination from the working group.

## E-2. REQUIRED TRAINING

a. The following are training requirements from FSEP.

<u>POSITION</u>	<u>REQUIREMENT</u>	<u>RESP AGENCY</u>
HRP & Family CID	Threat awareness briefing upon arrival and annually.	PMO, MI
Personnel traveling high threat areas	Briefed on threat and informed of provisions of DA Pam 190-52 (Personal Security Precautions Against Acts of Terrorism) prior to departure.	MI/unit Scty Personnel
Cdrs and Key Staff Personnel	Terrorist threat briefing -semi annual	MI, CID, PM
All	Threat and OPSEC awareness briefings - Annually or when necessary	OPSEC Officers
All	OPSEC awareness training during FTXs and during initial orientation	OPSEC Officers
Newly Assigned Personnel	OPSEC awareness training during initial orientation	G3, MI, CID, PM
CMT	Crisis management procedures, CBT/T response and operations. Exercise annually in conjunction with test of installation contingency plan.	Self
TMF	Training to maintain proficiency	TMF
All	Counteraction awareness training included in annual SAEDA briefing	MI
Operations, PM Intelligence Office	At a minimum a representative from each will have attended one of the following courses: Terrorism Counteraction Crs, United States Army Military Police School (USAMPS), Fort McClellan, Al, Dynamics of Internation'l Terrorism, Eglin AFB, Intelligence in Terrorism Counteraction, Fort Huachuca, AZ.	
Special Reaction Team (SRT)	At a minimum each member will have attended one of the following courses: SRT Trng Crs, USAMPS. An FBI or local police course that teaches SRT oriented special tactics. An installation SRT course that has the same or compatible program of instruction (POI) as above. Further training as stated in the FSEP.	

<u>POSITION</u>	<u>REQUIREMENT</u>	<u>RESP AGENCY</u>
HRP aide/escort	Weapons training, personnel protection training.	

b. The Army Terrorism Counteraction (CBT/T program) includes many of the same requirements as FSEP. In addition to those, AR 525-13 requires that:

(1) Commanders develop antiterrorism programs, threat briefings, and public affairs command information programs to inform and increase terrorism and personal protection awareness among military and civilian personnel and their family members.

(2) Hostage negotiators be trained.

E-3. RECOMMENDED TRAINING LEVELS - NO THREAT CONDITION. These are recommendations for fulfilling the requirements of the FSEP and AR 525-13 and for insuring that Fort Hood's CBT/T Program is effective through well trained personnel.

<u>ORGANIZATION</u>	<u>POSITION</u>	<u>COURSE(S)</u>
1. Cmd Group	Garrison Cdr	Senior Officer CBT/T Seminar (USAMPS) as director of CMT: Cmd Post Exercise (Fort Hood)
	SGS/Exec Svc Officer	Dynamics of Internat'l Terrorism (Hurlburt Field (USAF), FL)
	CG/DCG drivers	Evasive Driving for General Officer Drivers (USAMPS)
2. HQ Cmd	Ops Off/NCO	CBT/T on Military Installations (USAMPS)
3. DPIL	none	
4. FHIG	Trng Inspector	CBT/T on Military Installations (USAMPS)
5. Int Audit Division	none	
6. PAO	PAO	As CMT member: Cmd Post Exercise (Fort Hood)
	PAO-designated	As TMF member: Cmd Post Exercise (Fort Hood)
	Comm Relations Officer/Asst	CBT/T on Military Installations (USAMPS)
7. SJA	SJA	As CMT member: Cmd Post Exercise (Fort Hood)
	Admin Law Officer	CBT/T on Military Installations (USAMPS)
	Plans & Ops Officer	Legal Aspects of Terrorism Course (TJAGSA)
8. G1	none	
9. G2	CI Officer/NCO	Intelligence in CBT/T (Fort Huachuca)
	CI Analysis Off/NCO	Intelligence in CBT/T (Fort Huachuca) Dynamics of International Terrorism (Hurlburt Field (USAF), FL)

<u>ORGANIZATION</u>	<u>POSITION</u>	<u>COURSE(S)</u>
10. G3/PTM	G3/PTM	Senior Officer CBT/T (USAMPS) as CMT member: Cmd Post Exercise (Fort Hood)
	CBT/T Officer	Two of three: CBT/T on Military Intelligence (USAMPS), Intelligence in CBT/T (Fort Huachuca), CBT/T Instructor Course (CGSC)
	CBT/T/NCO	Dynamics of International Terrorism (Hurlburt Field (USAF, FL) Antiterrorism Instructor Qualification Course (USAJFKSWC)
	CONUS Contingency	CBT/T ON MILITARY INSTALLATIONS (USAMPS)
	CONUS Exercise Action Officer	Dynamics of International Terrorism (Hurlburt Field (USAD), FL)
	COC Officer in charge (OIC)	Dynamics of International Terrorism (Hurlburt Field (Usaf), FL.) Command Post Exercise (Fort Hood)
	COC NCO in charge (NCOIC)	Terrorism Counteraction on Military Installations (USAMPS) Command Post Exercise (Fort Hood)
11. G4	None	
12. G5	None	
13. AG	Dpty AG for Ops	CBT/T on Military Installations (USAMPS)
14. Aviation	HAAF & RGAAF OIC/ Ops Officer	CBT/T on Military Installations (USAMPS) Command Post Exercise (Fort Hood)
15. Chaplain	Garrison Chaplain	As Crisis Mgmt Team member: Cmd Post Exercise (Fort Hood)
16. Corps AMO	CAMO/Dpty CAMO	AIS Resource Protection (Nat'l Defense Univ, Washington D.C.)
17. Corps Signal		None
18. Corps Chemical		None
19. Corps Engineer		None
20. Surgeon	Corps Surgeon	As Crisis Mgmt Team member: Cmd Post Exercise (Fort Hood)
	Plans/Ops Officer	Terrorism Counteraction on Military Installations (USAMPS)
21. DCP	None	
22. DCCA	None	

<u>ORGANIZATION</u>	<u>POSITION</u>	<u>COURSE(S)</u>
23. DEH	Director	Senior Officer CBT/T Seminar (USAMPS) or Terrorism Seminar (CA Specialized Training Institute) as CMT member: Cmd Post Exercise (Fort Hood)  Emergency Mgmt Off CBT/T on Military Installations (USAMPS)
	Planning/Design Off	CBT/T design seminar/workshop/course (as available)
24. DOL	Director	as Crisis Mgmt Team member: Cmd Post Exercise (Fort Hood)
	Security Coordinator	CBT/T on Military Installations (USAMPS)
25. DOIM/USAISC	Director	as CMT member: Cmd Post Exercise (Fort Hood)
	Dpty or Ops Officer	CBT/T on Military Installations (USAMPS)
	Automation Security Officer	Computer Security (Essex Corporation)
26. DPCA	Director	as CMT member: Cmd Post Exercise (Fort Hood)
27. DRC	Training Officer	Antiterrorism Instructor Qualification Course (USAJFKSWC)
28. DRM	None	
29. DSEC	Director	Senior Officer CBT/T Seminar (USAMPS) or Intelligence in CBT/T (if seminar not available) as CMT member: Cmd Post Exercise (Fort Hood)
	Intel &Sec Specialist	Antiterrorism Instructor Qualification Course (USAJFKSWC)
	Tech Security Spec	Computer Security (Essex Corp)
30. DHS	see MEDDAC	
31. PM	PMO	Senior Officer CBT/T Seminar (USAMPS) as TMF/Task Force Cdr: Cmd Post Exercise (Fort Hood)
	PMO Designated rep	as CMT member: Cmd Post Exercise (Fort Hood)
	Ops Officer	CBT/T on Military Installations (USAMPS) as TMF member: Cmd Post Exercise (Fort Hood)
	Phys Sec Officer	Terrorism Course (CA Specialized Training Institute)
	SRT	SRT Course (USAMPS or Essex Corp)

<u>ORGANIZATION</u>	<u>POSITION</u>	<u>COURSE(S)</u>
	SRT OIC	As member of TMF: Cmd Post Exercise (Fort Hood)
32. MEDDAC	Plans, Ops, and Planning Chief/Asst	CBT/T on Military Installations (USAMPS)
	Emergency Medical Tm	As members of TMF Cmd Post Exercise (Fort Hood)
33. DENTAC	None	
34. MSCs		
Divisions:	HRP drivers	Evasive Driving for General Officer Drivers (USAMPS)
	MP Co Officer	Executive Protective Services (USAMPS or Essex Corp)
	MP Co Off/Asst	Antiterrorism Instructor Qualification Course (USAJFKSWC). CBT/T on Military Installations (USAMPS)
	CG designated rep	As CMT member: Cmd Post Exercise (Fort Hood)
MSCs:	MSC Ops Off/Asst	Antiterrorism Instructor Qualification Course (USAJFKSWC) and Dynamics of International Terrorism (Hurlburt Field (USAF), FL) or CBT/T on Military Installations (USAMPS)
	MSC Intel Off/Asst	Intelligence in CBT/T (Fort Huachuca)
35. USACIDC	Commander	As CMT member: Cmd Post Exercise (Fort Hood)
	Hostage Negotiator	Hostage Negotiations Course
	Designated Reps	As members (2) of TMF Cmd Post Exercise (Fort Hood)
36. TEXCOM	Security Officer	Antiterrorism Instructor Qualification Course (USAJFKSWC) or Dynamics of Internat'l Terrorism (Hulburt Field (USAF), FL)
	CG's driver	Evasive Driving for General Officer Drivers (USAMPS)
37. 902d Resident Office	Special Agent in Charge	As CMT Member: Cmd Post Exercise (Fort Hood)
	Special Agent	As TMF member: Cmd Post Exercise (Fort Hood)

**SECTION II - RECOMMENDED TRAINING LEVELS PRIOR TO INCREASED THREAT**

E-4. RECOMMENDED TRAINING LEVELS - INCREASED CONUS THREAT. These recommendations become effective if an increase in terrorist threat and activity occurs in the United States, but prior to THREATCON implementation if possible, as determined by threat analysis and designated by the Commander, III Corps and Fort Hood.

<u>ORGANIZATION</u>	<u>POSITION</u>	<u>COURSE(S)</u>
1. Cmd Group	CG & DCG	Executive Survival (Essex Corp), General Driver Evasive Driving Course (USAMPS)
	CG/DCG driver	Conventional Personal Defense (Essex Corp) Handgun Combat Shooting (Essex Corp)
	SGS/ Chief Exec Svc	Security in Public Institutions (Essex Corp) Individual Terrorism Awareness Course (USAMPS) Executive Protective Services (USAMPS or Essex Corp)
	Dpty CofS	Senior Officer CBT/T Seminar (USAMPS)
2. HQ Cmd	Exec Officer	Security in Public Institutions (Essex Corp)
3. DPIL	Exec Officer	CBT/T on Military Installations (USAMPS)
4. FHIG	None	
5. Int Audit Division	None	
6. PAO	None	
7. SJA	None	
8. G1	None	
9. G2	None	
10. G3/PTM	None	
11. G4	None	
12. G5	None	
13. AG	None	
14. Aviation	None	
15. Chaplain	Garrison Chaplain	Terrorism Seminar (CA Specialized Training Institute)
16. Corps AMO	None	
17. Corps Signal	None	
18. Corps Chemical	None	
19. Corps Engineer	None	
20. Surgeon	None	

<u>ORGANIZATION</u>	<u>POSITION</u>	<u>COURSE(S)</u>
21. DCP	None	
22. DCCA	None	
23. DEH	Asst Dir of Ops	CBT/T on Military Installations (USAMPS)
	Chief/Asst Plans &	Terrorism Course (CA Specialized Services Training Institute)
24. DOL	Supply & Services Officer/Asst	Terrorism Course (CA Specialized Training Institute)
	Fuel Distribution System Foreman	Terrorism Course (CA Specialized Training Institute)
25. DOIM/USAISC	None	
26. DPCA	Ops Officer	Security in Public Institutions (Essex Corp) <b>or</b> Terrorism Course (CA Specialized Training Institute)
	Installation Club	Same as above
	System Supervisor	Same as above
	Morale Support Activities Supervisor	Institutions Terrorism Course (CA Specialized Training Institute)
27. DRC	None	
28. DRM	None	
29. DSEC	Intel & Security	Dynamics of Internat'l Terrorism (Hulburt Field (USAF), FL) <b>or</b> Intelligence in CBT/T (Fort Huachuca)
30. DHS	None	
31. PM	None	
32. MEDDAC	None	
33. DENTAC	None	
34. MSCs		
Divisions:	CG	Executive Survival (Essex Corp) General Officer Evasive Driving Course (USAMPS)
	CG drivers	Unconventional Personal Defense (Essex Corp) Handgun Combat Shooting (Essex Corp)
	SGS/Exec Svc	Dynamics of International Terrorism (Hulburt Field (USAF), FL)
	SGS/Aide	Individual Terrorism Awareness Course (USAJFKSWC)

<u>ORGANIZATION</u>	<u>POSITION</u>	<u>COURSE(S)</u>
	MP (2 per MP Company)	Executive Protective Services (USAMPS or Essex Corp)
All MSCs:	Ops Off/Asst down to Battalion level	Antiterrorism Instructor Qualification Course (USAJFKSWC)
	Intl Off/Asst down to Battlaion level	Intelligence in CBT/T (Fort Huachuca)
35. USACIDC	None	
36. TEXCOM	CG	Executive Survival (Essex Corp) General Officer Evasive Driving Course (USAMPS)
	CG Driver	Unconventional Personal Defense (Essex Corp) Handgun Combat Shooting (USAMPS)
37. 902d Resident Office	None	

**APPENDIX F**

**SUMMARY OF FORSCOM SECURITY ENHANCEMENT PLAN**

F-1. The FSEP was published in April 1985 to standardize selected anti and counterterrorism measures and procedures throughout FORSCOM. The intent is to uniformly and effectively deter and/or neutralize potential terrorist activity should an incident occur.

F-2. a. The FSEP includes four chapters: Introduction, Threat, Active Component (AC) Standards, and United States Army Reserve (USAR). The standards specified in this plan are minimum requirements. Deviations below the standard require approval from FORSCOM. There are basic standards that must be established regardless of the threat level and incremental standards as the threat increases. Functions addressed under AC standards include high risk personnel/very important person (HRP/VIP) security, SRT, MEVAs, communications, intelligence, and operations. For each function, the threat level, standards, proponent, reference, and E-date (Latest date to comply) are listed.

b. The CBT/T working group monitors the status of FSEP implementation at Fort Hood.

APPENDIX G

**SUMMARY OF OPLAN READY GO**

G-1. The purpose of III Corps and Fort Hood Special Threat OPLAN (Short Title: READY GO), 31 Mar 86, with chg 1, 21 Oct 87, is to provide a means to contain and eliminate special threat situations on post that are beyond the capability of normally committed MP patrols.

G-2. READY GO is a standard five paragraph order with designated responsibilities. The OPLAN addresses reaction to a variety of special threat situations. This plan is in compliance with the FSEP, 12 Apr 85.

G-3. READY GO is the CG's counterterrorism plan.

## APPENDIX H

## ACCESS CONTROL PLAN

## SECTION I - GENERAL

H-1. The access control plan is the CG's plan to protect the Fort Hood cantonment areas. Inherent in his responsibility as the CG III Corps and Fort Hood, is the authority to control access to the installation and protect MEVA. This authority is derived from his responsibilities to protect and secure personnel, government property, and information of a sensitive nature. The degree of implementation of this plan will be directed by the CG as the situation may require.

## H-2. Access Control Plan

a. The access control plan is geared toward combating terrorist acts or an imminent threat to the installation. MP tactical units are used, until THREATCON CHARLIE.

b. Assumptions. The implementation of the access control plan is a buildup process which necessitates the support of intelligence assets in providing the type of information that would lead the CG to raise the THREATCON level above normal. Intelligence information will be disseminated through G2/S2/DSEC and COC channels to the appropriate level of command. This information will also serve as a warning to MSCs that a change in THREATCON level may occur and that a review of counterterrorism plans is necessary. This concept is particularly important in regard to personnel who are required to deploy for implementation of the access control plan.

## H-3. Concept of the Operation.

a. The access control plan is an installation plan which has been developed to control access to Fort Hood's cantonment areas. At THREATCON CHARLIE or on order of Commander, III Corps tactical units are required to deploy to ACPs and implement measures as directed in this regulation to control traffic, identify incoming/outgoing personnel, search packages and closed containers, and implement any other measures for identification/screening as necessary.

b. Detailed requirements for implementation of the access control plan are found in Sections II, III and IV.

## H-4. Responsibilities.

## a. ACofS, G3/PTM, III Corps:

(1) Announce THREATCON level and disseminate this information to BC's and installation staff.

(2) Direct the implementation of the access control plan as ordered by the CG, III Corps and Fort Hood. A minimum of three hours is necessary to assemble, organize, and equip personnel prior to execution of this plan.

(3) Increase or decrease the THREATCON level as directed.

(4) Terminate the access control plan as appropriate.

## b. III Corps PM

(1) Develop a plan to allow for the partial or complete closure of Fort Hood cantonment areas, which includes measures to be taken at the ACPs and operational diagrams depicting MP positions for controlling access/egress IAW the guidelines established in this plan. Provide a copy of the plan to units involved.

(2) Upon implementation assume duties as Task Force Commander of TMF.

(3) Notify local law enforcement agencies of the access control plan implementation and implications for their communities.

c. Commanders, III Corps BC's:

(1) Provide personnel according to Sections II and IV.

(2) Prepare a supporting plan to sustain this operation indefinitely.

(3) Execute BC plans according to declared THREATCON.

(4) On order security forces at Sections II and IV are prepared to deploy within three hours upon declaration of THREATCONs CHARLIE or DELTA.

(5) As soon as personnel are ready to deploy, contact the III Corps MP station by telephone (287-4001/2176/2177/2178) or by radio in order to receive further instructions.

(6) Establish control through respective EOCs to III Corps EOC.

(7) Block designated access points for closure at Sections II and IV, until DEH can position temporary barricades. Keep one soldier at each blocked access point to direct traffic to the appropriate ACP.

(8) Actions to be taken at the ACPs will be IAW the declared THREATCON level (Section III); appendix K (Use of Force) , and appendix M (Inspection Procedures).

(9) Additional actions may be required at the ACPs as directed by the CG. Guidance for ACP actions will be IAW appendix K (Use of Force) and appendix M (Inspection Procedures).

(10) Be prepared to execute OPLAN READY GO on order.

d. DEH.

(1) Develops and maintains traffic circulation control plan for each ACP, to include barrier material requirements and emplacement procedures.

(2) Coordinates with III Corps PM to be sure that traffic circulation control plans support MP traffic control requirements and develop ACP diagrams.

(3) Execute barrier emplacement plan for closed ACPs at THREATCON CHARLIE (see Sections II and IV).

(4) Upon notification that the access control plan is going to be implemented, be prepared to provide the engineer support necessary to conduct this operation.

(5) The following list indicates the equipment necessary for support. The list is not inclusive and requirements may change based on the threat.

(a) 750 traffic cones

(b) Wooden/synthetic barricades (number is dependent on situation)

(c) Heavy barricades (cement/heavy metal), which can temporarily seal the necessary ACPs IAW Sections II and IV.

(d) Check point signs.

(e) Warning lights.

(f) Maintain sufficient number of personnel and necessary equipment which may be required to make minor modifications on terrain adjacent to or at the ACPs.

(6) The equipment listed above will be stored by DEH in order to facilitate rapid emplacement and collection.

f. PAO.

(1) Upon notification that the access control plan is to be implemented, establish an information center to provide support to the news media. Inquiries for information on this operation will be directed to the information center.

(2) The PAO will provide a representative to the Corps EOC.

(3) The PAO controls media access to scene of an incident.

(4) The PAO coordinates release of information with other key federal agencies.

(5) In coordination with the Task Force Commander, make sure the news media is kept abreast of the current situation, as appropriate.

g. DCP. Notify labor unions about road closures and ACPs listed in Section II. Upon notification that the access control plan will be implemented, inform the labor unions with as much notice as possible.

h. Coordinating Instructions.

(1) If the need for response is less than the three hours required to prepare the MP tactical units for deployment, then MP road patrols will be dispatched to provide the support. This condition must be avoided, only used in emergencies and can only sustain the operation temporarily since only one or two units would be left to patrol the installation. The absence of barricades, cones, etc will seriously impair mission accomplishment. This capability would only support Fort Hood's main cantonment area.

(2) The number of personnel required is listed in Sections II and IV.

(3) Units must be prepared to sustain the operation indefinitely.

(4) This plan will be tested as directed by the CG, III Corps and Fort Hood.

#### H-5. Service Support.

a. Organic unit is responsible for providing the following:

(1) Transportation

(2) FM radios

(3) Establishment of rotating shifts

(4) Mess support

(5) Supervisory personnel

b. DEH must be prepared to provide the equipment necessary to activate the ACPs (paragraph H-4, d) to each access point.

#### H-6. Command and Signal.

a. Control headquarters is through BC EOC's to III Corps EOC, upon declaration of THREATCON CHARLIE.

- b. Deployed units will use FM frequencies in appendix L.
- c. Checkpoint numbers will be used as call signs.
- d. Location of ACPs will not be announced over the radio nets.

## SECTION II - ACCESS CONTROL POINTS (ACPs)

H-7. This section gives the location of ACPs for Main Fort Hood, West Fort Hood, and North Fort Hood. The number of personnel needed is estimated, based on the need to provide circulation control and the varied missions under THREATCON CHARLIE or DELTA. Entrances shown to be closed at THREATCON ALPHA and THREATCON CHARLIE will be manned by each BC until the DEH or PM can execute physical closure (minimum of three soldiers at each closure).

- a. Entrances to close at THREATCON ALPHA or on order:

- (1) Garth Drive at post boundary.
- (2) Venable Drive at Ball Field Road.
- (3) Wales Street at US 190.
- (4) Kildea Street at US 190.
- (5) Turkey Run Road at west side of Clarke Road.
- (6) Ammo Road behind Central Texas College (CTC) (PK131425).
- (7) Block access to Clear Creek Park from US 190 and block south-east access roads to Clear

Creek Park.

- b. Entrances to close at THREATCON CHARLIE or on order:

- (1) Central Drive at 8th Avenue (post boundary).
- (2) Venable Drive (East) at Business 190.
- (3) Clement Drive at Clarke Road.
- (4) Washington Street (East) at the south side of Ammo Road.
- (5) Black Gap Road at the cattle guard and tank trail.
- (6) East Gate (at Tank Destroyer and Fort Hood Street).
- (7) Copperas Cove Road at west low water crossing.
- (8) Mohawk Road at Oakalla Road.
- (9) Gray Drive at south RGAAF entrance.
- (10) 24th Street (west) & Hwy 36 (North Fort Hood (NFH)).
- (11) 21st Street (west) & Hwy 36 (NFH)
- (12) 18th Street (west) & Hwy 36 (NFH)
- (13) 16th Street (west) & Hwy 36 (NFH)

- (14) 12th Street (west) & Hwy 36 (NFH)
- (15) Ave A/21st Street (east) & Hwy 36 (NFH)
- (16) 18th Street (east) & Hwy 36 (NFH)
- (17) 16th Street (east) & Hwy 36 (NFH)

c. ACPs to man at THREATCON CHARLIE, THREATCON DELTA or on order (Primary ACP's):

<u>Entrance</u>	<u>MSC Responsible</u>	<u>Personnel Required CHARLIE/DELTA</u>
(1) Main Gate	1CD	30/50
(2) Clear Creek	1CD	30/50
(3) Warrior Way	6CB (AC)	30/50
(4) East Range Road	6CB (AC)	15/23
(5) RGAAF North Entrance	504 MI	30/50
(6) West Range Road	1CD	15/23
(7) Clarke Road (north side US 190)	31 ADA	13/21
* (8) 79th St at US 190	COSCOM	15/20

\* This entrance only for emergency vehicles, wide or oversize loads, and specifically designated key personnel.

d. Isolated Housing Area ACP's to be manned at THREATCON CHARLIE, THREATCON DELTA, or on order. ACP's will only be manned based on specific threat to housing areas.

(1) Venable Village (west)	3 SIG	8/12
(2) Hoover Hill & US 190	3 SIG	8/12
(3) Hoover Hill & Hwy 195	3 SIG	8/12
(4) Liberty Village	31 ADA	5/9
(5) Montague Village (Ovnard Blvd & Clarke)	504 MI	9/13

e. The following North Fort Hood ACP's will be manned on order by US Army National Guard or USAR forces occupying NFH.

(1) 12th Street & East Range Road (NFH)	5/9
(2) East & West Range (NFH)	5/9
(3) 15th Street (west) & Hwy 36 (NFH)	5/9
(4) 15th Street (west) & Hwy 36 (NFH)	5/9
(5) 24th Street (east) & Hwy 36 (NFH)	5/9
(6) 15th Street (east) & Hwy 36 (NFH)	5/9

f. Breakdown by unit per eight hour shift:

	<u>CHARLIE</u>	<u>DELTA</u>
1CD	75	123
3SIG	24	36
6CBAC	45	73
31ADA	18	30
504MI	39	63
COSCOM	15	20
— — —		
TOTAL	216	345

**SECTION III - REQUIREMENTS AT ACPs**

H-8. The requirements listed below are the minimum objectives while providing access control to Fort Hood. These requirements are directly related to each level of THREATCON. The threat may require the implementation of additional/special actions.

H-9. These actions are cumulative as the THREATCON level increases from THREATCON ALPHA through THREATCON DELTA, or at the level of THREATCON implemented. (NOTE: THREATCONS are not progressive. Any THREATCON can be initiated without going through the lower level(s).)

H-10. Normally, these requirements are directed at vehicles entering the installation. If the requirements are to include outbound traffic, units will be notified as part of their special instructions.

a. THREATCON ALPHA:

- (1) Control flow of traffic.
- (2) REDUCE NUMBER OF VEHICULAR ACCESS POINTS.
- (3) Establish random spot ID checks at ACPs.
- (4) Be alert for suspicious vehicles or personnel; stop suspicious vehicles/personnel and require personal identification.
- (5) Be prepared to implement additional measures as directed.

b. THREATCON BRAVO:

- (1) Control flow of traffic.
- (2) Increase number of random spot ID checks at ACPs.
- (3) Be alert for suspicious vehicles or personnel; stop suspicious vehicles/personnel and require personal identification.
- (4) Be prepared to implement additional measures as directed.

c. THREATCON CHARLIE:

- (1) Control flow of traffic.
- (2) Limit ACPs to absolute minimum.
- (3) Strictly enforce control of entry and search 50% of vehicles (or as directed). Personnel without appropriate identification will not be permitted entry. ACPs are manned continuously or until relieved from duty.

- (4) Inspect trunks of vehicles which are stopped for personnel ID checks.
- (5) Inspect cargo trucks, regardless of whether they are part of the 50% inspection or not.
- (6) Be prepared to implement additional measures as directed.

d. THREATCON DELTA:

(1) Strictly enforce control of entry and search 100% of vehicles. Personnel without appropriate identification will not be permitted entry. The search of the vehicle includes closed compartments of the vehicle.

(2) Search suitcases, briefcases, packages, etc.

(3) Be prepared to implement additional measures as directed.

H-11. A serious incident at an ACP is reported first to the PM, then through the BC EOC to the III Corps EOC. The purpose is to reduce the response time for deployment of MP quick reaction forces. Communication is through tactical FM radio. Be prepared to execute additional measures as directed.

APPENDIX I

**BASE CLUSTER/MAPS**

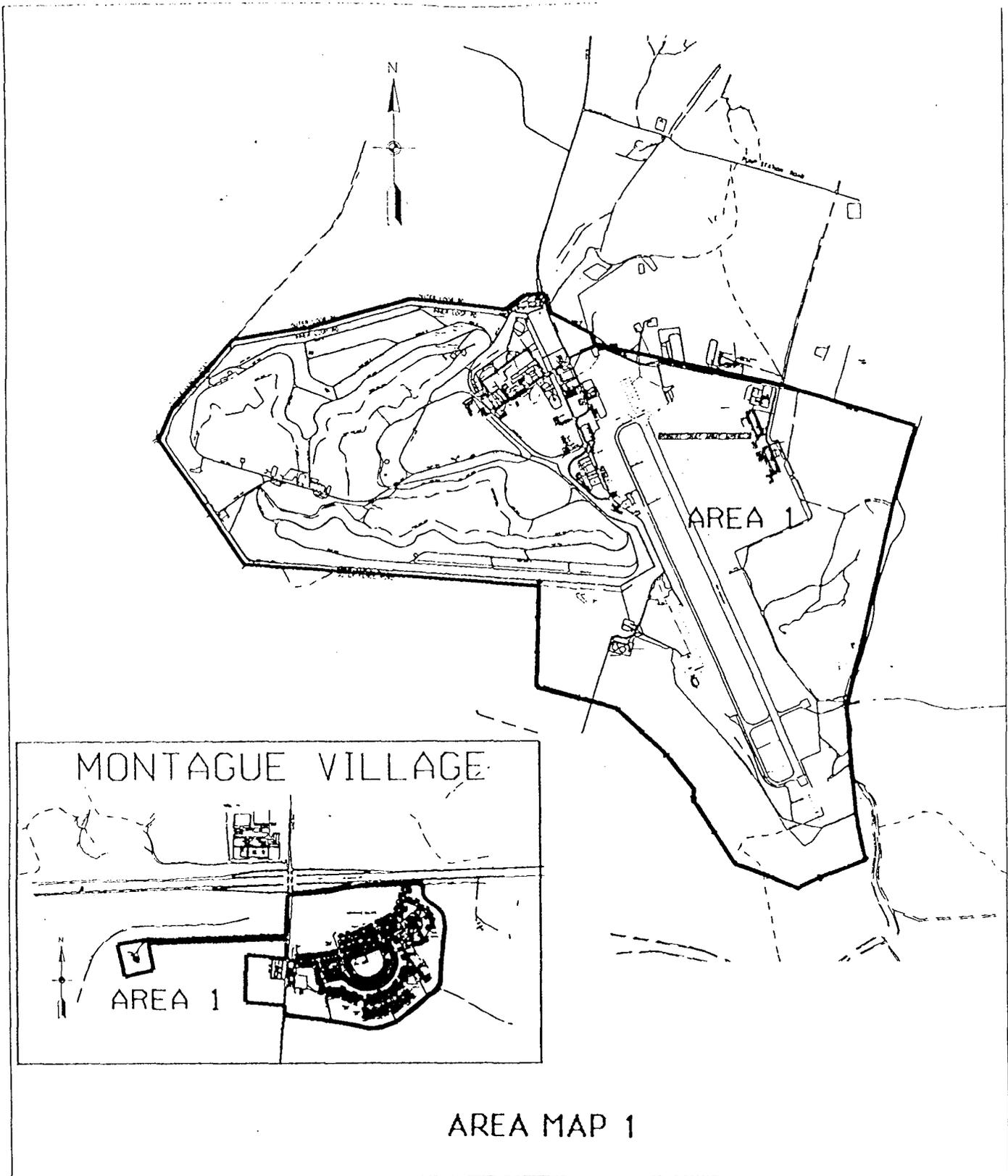
SECTION I - LISTING

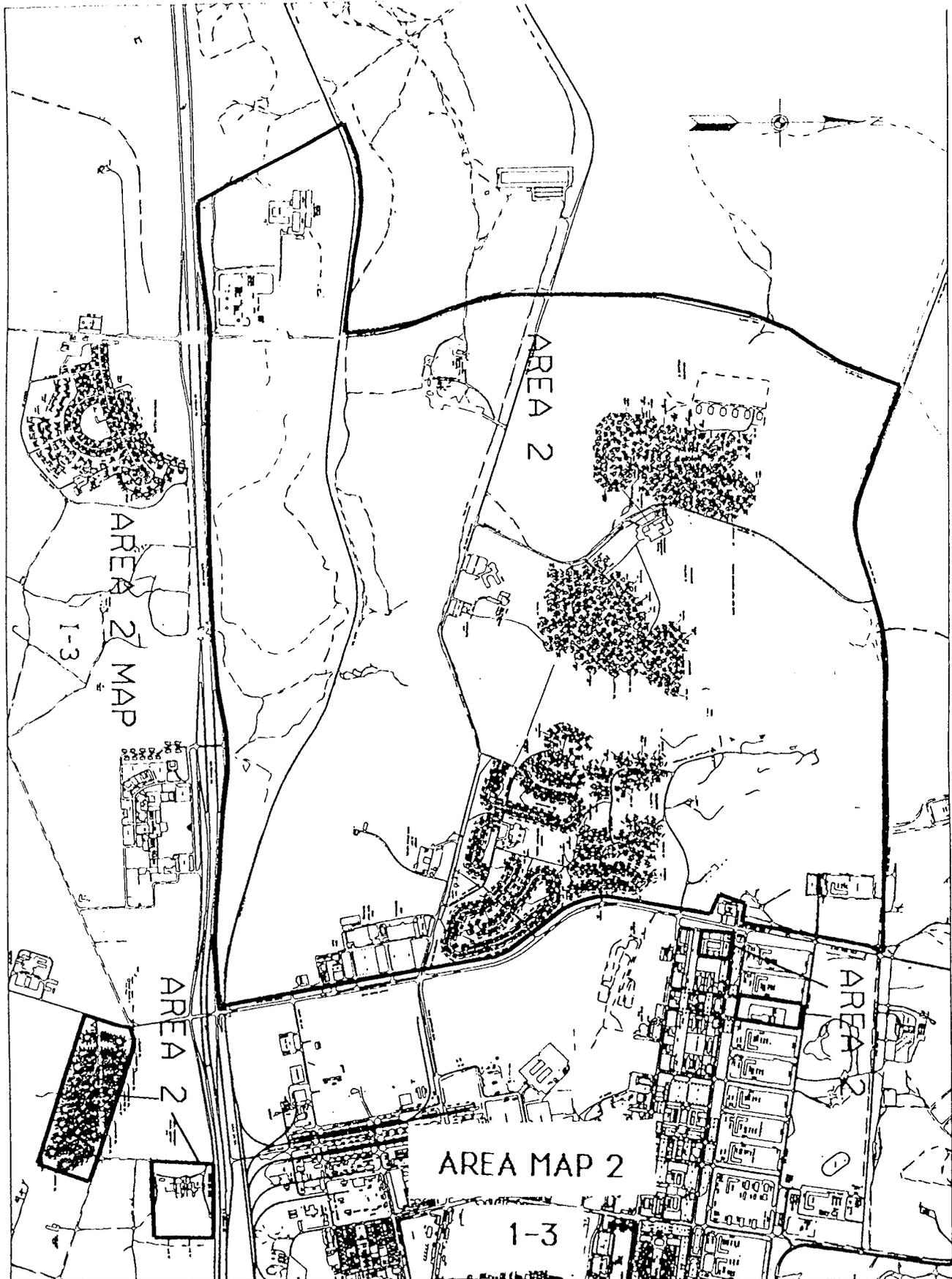
- Area 1 - 504th MI Bde
- Area 2 - 31st ADA
- Area 3 - 1st CD
- Area 4 - 13th COSCOM
- Area 5 - 3rd Sig Bde
- Area 6 - Headquarters Command (Bldgs 1001, 11, 13)
- Area 7 - TBD
- Area 8 - 6 CB (AC)
- Area 9 - North Fort Hood

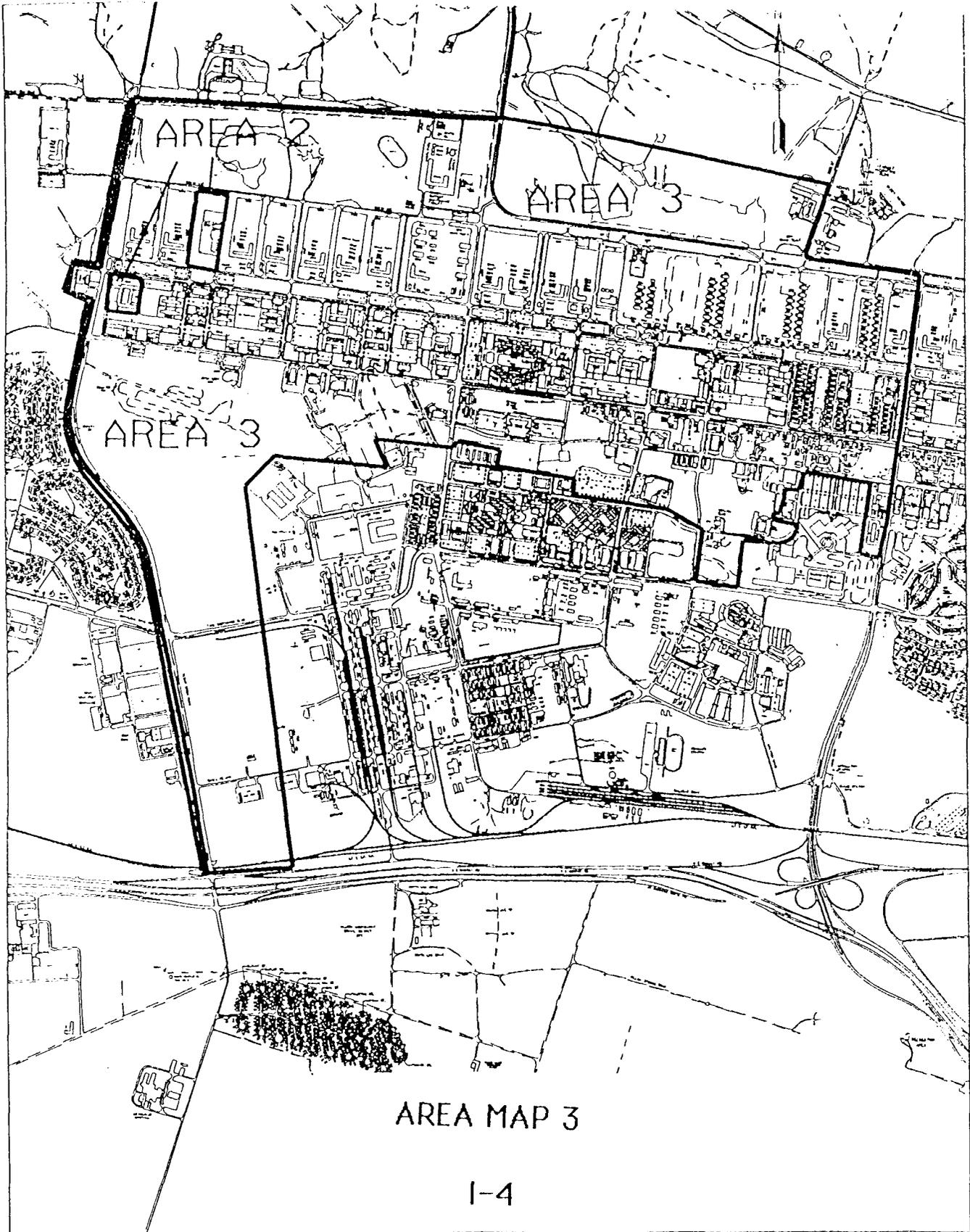
**SECTION II - MAPS**

This series of maps of Fort Hood depict the MSC BC. A larger and more detailed pair of Fort Hood maps is available for review. POC is G3, CBT/T Action Officer 287-6525/6336.

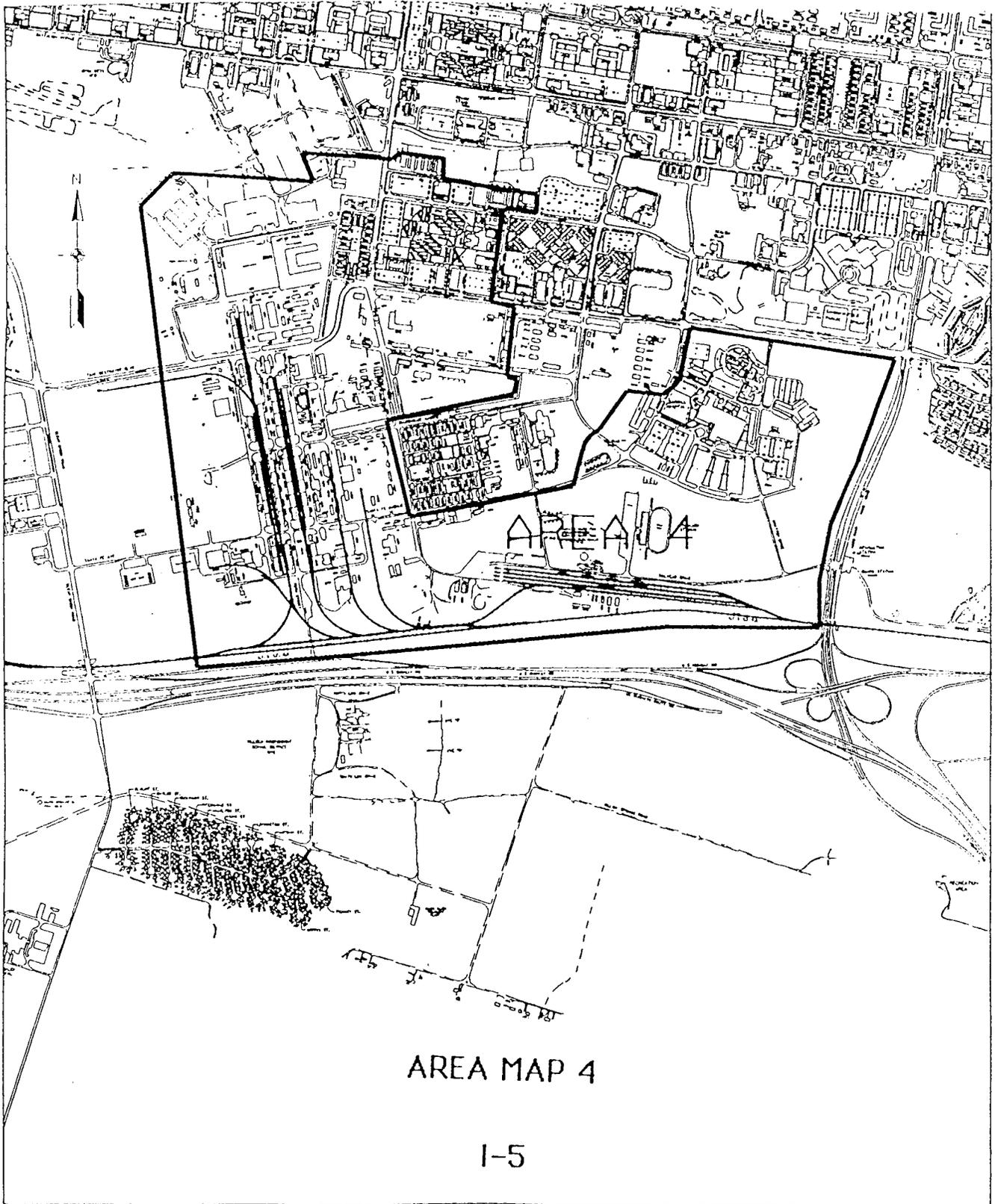
Map	Page
Area 1	Map - I-2
Area 2	Map - I-3
Area 3	Map - I-4
Area 4	Map - I-5
Area 5	Map - I-6
Area 6	Map - I-7
Area 7	Map - I-8
Area 8	Map - I-9
Area 9	Map - I-10





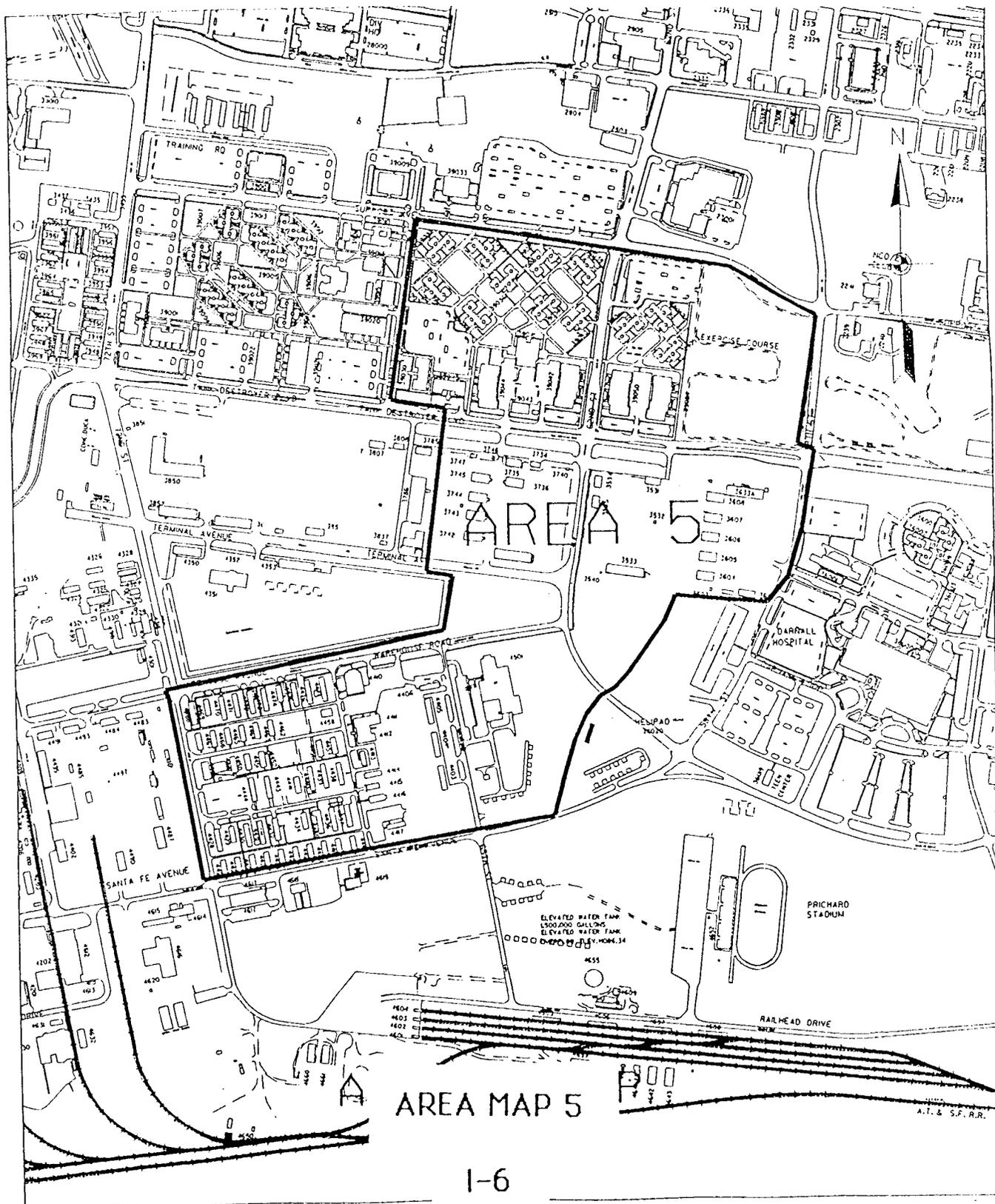


AREA MAP 3



AREA MAP 4

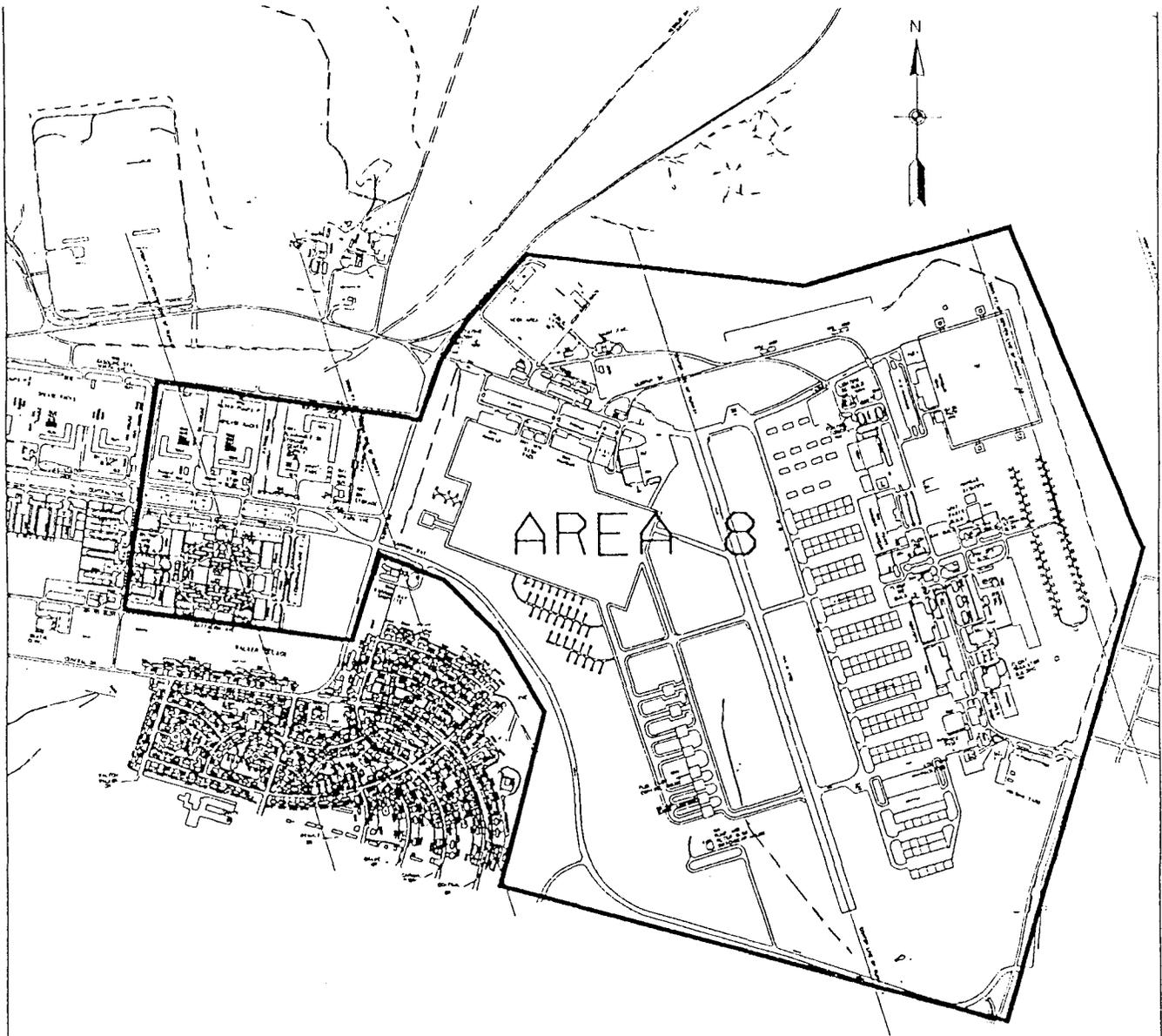
I-5



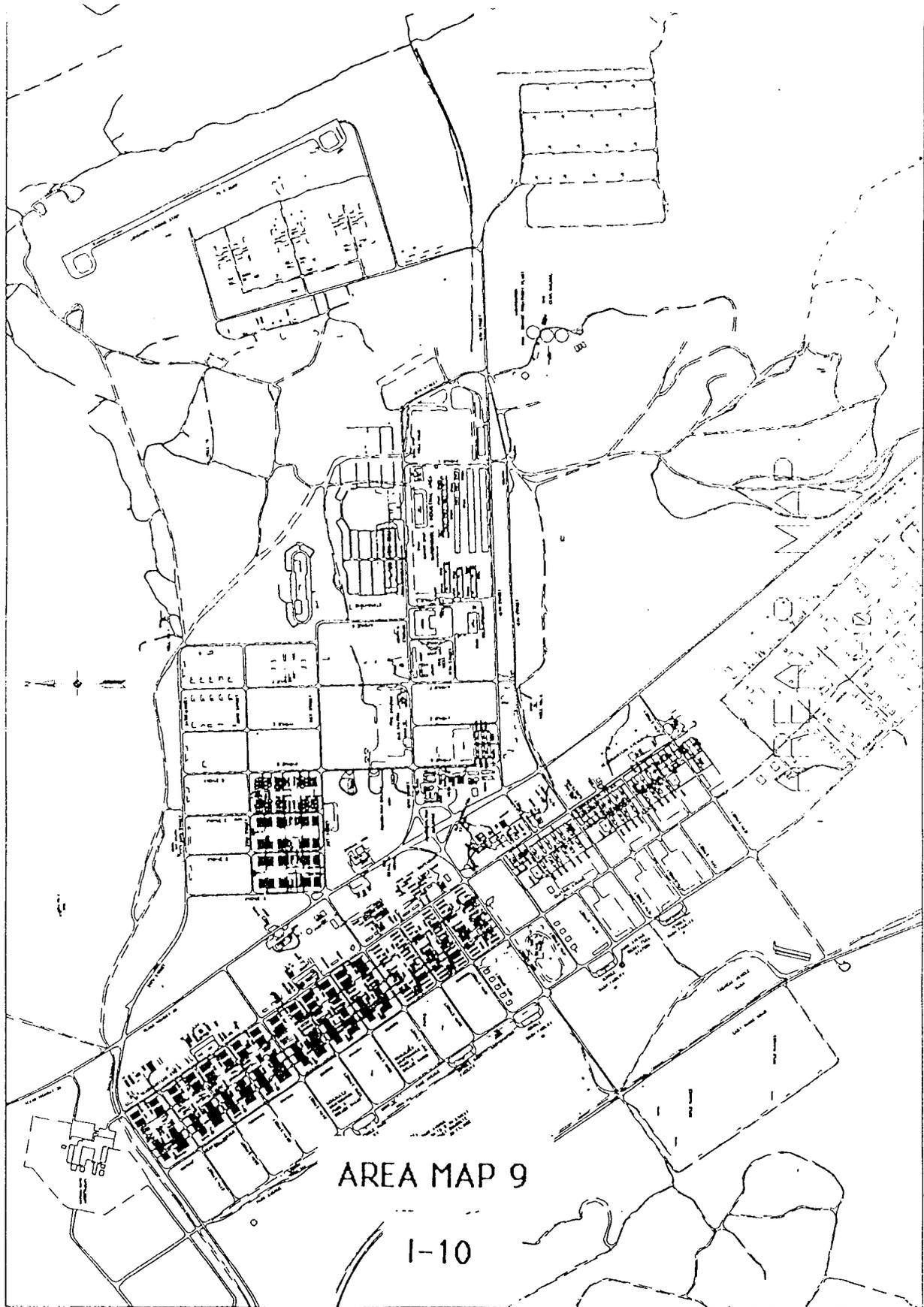




AREA MAP 7



AREA MAP 8



## APPENDIX J

**BATTLE BOOKS**

J-1. BCC's will prepare battle books for their BCs. Battle books will be prepared so they are relative to actions which must start, stop, or be coordinated for each specified THREATCON. Battle books will consist of, at a minimum the following appendices:

Appendix A	Base Responsibilities
Appendix B	Emergency Operations Center Operations and Layout
Appendix C	Communications
Appendix D	Overall Base Cluster Diagram
Appendix E	Force structure (will include an identification of changes to force structure command responsibilities relative to change in given THREATCON levels)
Appendix F	Ammunition
Appendix G	Meva and ACP sites - will include at a minimum the following: Directions to site Site diagrams Guard force requirements and responsibilities Guard force reporting procedures Communications Special instructions
Appendix H	Special instructions for use of force and conducting inspections/searches.

J-2. Battle books will be routinely reviewed for effectiveness and feasibility of implementation. A copy of the BC battle book will be provided to III Corp, G3 Operations Division ATTN: AFZF-GT-PO for review and are an inspectable item.

J-3. Upon mobilization BC battle books will be passed to unit occupying the BC. Responsibility for the BC, as far as CBT/T, will be assumed upon receipt of battle books and deployment of the unit designated herein as BCC. If the unit that is to occupy the BC has not arrived at the time the BCC deploys, battle books will be turned in to the Corps' EOC. The EOC will pass the battle books to the arriving units.

Should an incident occur between the time the BCC deploys and the next unit arrives the Corps G3 will task a unit to take over the protection of the BC and provide that unit the battle books for the BC.

## APPENDIX K

**USE OF FORCE FOR SECURITY PERSONNEL**

K-1. Soldiers that are assigned security duties, either guarding critical facilities or controlling the access of traffic at the gates may be issued ammunition. If needed, only one magazine of ammunition will be issued, which will be carried in the ammunition pouch. Weapons will be cleared by the NCOIC at the beginning and end of each shift. Based on local threat conditions, the NCOIC may direct that the magazine be inserted. Soldier's will not insert a magazine without the permission of that NCOIC, unless use of deadly force is allowed (see below).

K-2. The following criteria extracted from AR 190-14, must be briefed to and understood by each soldier performing guard duties with live ammunition.

a. Security personnel will use only the minimum amount of force necessary to fulfill assigned duties. Only as a last resort will deadly force be used.

b. In evaluating the degree of force required, the following options should be considered in the order listed, when they are available.

(1) Verbal persuasion

(2) Unarmed defense techniques

(3) Chemical aerosol irritant projectors

(4) MP club

(5) Military working dogs

(6) Presentation of deadly force capability (showing the weapon and the intent to use it without actually firing).

(7) Deadly force (that force which a person uses with the purpose of cause or which the person knows, or should know, will create a substantial risk of causing death or serious bodily harm).

c. Deadly Force

(1) Use deadly force only under conditions of extreme need and as a last resort, when lesser means have failed or cannot reasonably be used. Use deadly force only under one or more of the following circumstances.

(a) Self-Defense. When in imminent danger of death or serious injury.

(b) To prevent sabotage or theft of property (such as operable weapons or ammunition) which, in the hands of an unauthorized person, presents a substantial threat of death or serious bodily harm to others.

(c) When directed by the lawful order of a military superior.

(2) Should use of a firearm in any of the circumstances described above be necessary, observe the following precautions when possible to do so consistent with the prevention of death or serious bodily harm:

(a) Give an order to halt, if practical.

(b) Do not fire if shots are likely to harm innocent bystanders.

(c) When possible, aim to disable, rather than to kill where this degree of accuracy can be affected without resulting in a hazard to the guard or innocent bystanders.

K-3. Guard commanders must record pertinent information concerning the briefing in their duty log to include names, date, and time of the briefing.

## APPENDIX L

**BASE CLUSTER SIGNAL INSTRUCTIONS**

L-1. Upon implementation of the Fort Hood CBT/T program each BC and III Corps will go to the appropriate Signal Operating Instructions (SOI) for that time period and use the below listed nets to communicate with their guard and ACP forces.

a.	III Corps	Corps Cmd Net
b.	1 CD	Div Cmd Net
c.	TBD	Unit Cmd Net
d.	6 CB (AC)	Bde Cmd Net
e.	13 COSCOM	COSCOM Cmd Net
f.	3 SIG	Bde Cmd Net
g.	504 MI	Bde Cmd Net
h.	31 ADA	Bde Cmd Net
i.	HQ Cmd	Cmd Net

L-2. At THREATCON BRAVO BC signal officers will prepare FH Form 105-X1 (Communication Service Request) for the appropriate telephone equipment needed at their respective ACP's and/or other locations. Coordinate with DOIM Telephone Division, for activating the request at THREATCON CHARLIE. BC OPLANS should address planning for telephone setup from the phone drop to the ACP/other locations. Planning may include cellular telephone backup usage until primary telephones are operational.

L-3. Motorola radios (hand held 'brick') should be considered as additional means of communication. BC's with these radios should incorporate their usage in their BC communication plans.

L-4. Mobile Subscriber Equipment (MSE) will be installed on order. This is dependent on the number of Mobile Subscriber Radio Telephone (MSRT) subscribers.

L-5. Emergency communications with the MP station will be conducted on FM frequency 45.00 Mhz.

## APPENDIX M

**INSPECTION/SEARCH PROCEDURES PART I, ACCESS CONTROL POINTS (ACP'S) GUIDANCE**

M-1. Situation. The Fort Hood Installation Readiness posture may be elevated to THREATCON CHARLIE. As a result, the CG has directed that units be prepared to conduct gate checks IAW this regulation. The CG has signed letters of authorization for the searches and inspections to be conducted under each THREATCON level.

M-2. Mission. On orders, at locations specified by the CG, implement gate checks. Every other vehicle inbound will be inspected for contraband and to be sure that only authorized personnel are allowed on the installation.

M-3. Execution:

a. Personnel will be briefed and given assignments and Use of Force briefings prior to arriving at the gate.

b. On order, begin security operations at the specified gates.

- Upon approach to the gate, vehicles will be directed towards the processing area, guided into a lane and stopped.

- Each lane will have at least two soldiers:

- Soldier #1 will greet the driver and ask for military/DA civilian ID card and driver's license. Soldier #1 will then ask occupants for military/DA civilian ID card. If they have none, he will then ask for some form of picture identification. ID cards/driver's licenses will be checked for valid dates and personnel visually verified against ID photo. Soldier #1 will then ask the destination/nature of business on post if the driver or occupants are not military or DA civilians.

- Soldier #2 will stand on the right, or passenger side of vehicle, and watch the actions of occupants. Soldier #2 will observe the actions of the occupants and look into the vehicle for crates, boxes, briefcases, or other closed containers. Soldier #2 will assist in gathering occupants ID if necessary.

- Both soldiers will search by looking in windows of vehicle. Occupants will be asked to open closed containers including, but not limited to: boxes, briefcases, bags, glove compartment, and tape cases, etc.

The driver will then open any trunk or hatchback and the soldiers will again check closed containers.

c. If the driver is military or DA civilian and is required to have a post decal but does not, he/she will be directed to vehicle registration at Main Gate near the information booth.

d. If a civilian refuses inspection, he/she will be refused entry on post and be escorted out the gate. The full name and address of the person will be recorded and submitted to the MP.

e. If the driver does not have a driver's license, he will park the vehicle at the nearest convenient location and not be allowed to drive. If an occupant possesses a license, they may drive if the driver allows it.

f. Photograph ID's will match the person it belongs to.

g. ID cards/licenses will be checked to make sure they are not expired.

h. If explosives, weapons, or ammunition are found, detain occupants for MP arrival. Do not allow anyone to come near the suspected items expect MP or explosive ordnance disposal (EOD) personnel.

M-4. Service and Support.

a. Uniform. Battle dress uniform (BDU) with appropriate cold/wet weather gear, road guard vests, flashlights.

b. Equipment. Barricades and traffic cones will be prepositioned. Chemical lights will be provided by unit tasked.

c. Personnel. Support and technical advice from the PMO will be through an NCOIC/PM representative who will be available through the MP Desk Watch Commander, MP patrols will respond if needed. CID and SJA will be on standby to provide assistance as needed.

#### M-5. Command and Signal

Command - See BC OPLAN

Signal - See appendix L.

ACP OIC/NCOIC will conduct hourly communication check with the MP station.

### **INSPECTION/SEARCH PROCEDURES - PART II MEVA/GUARD/ROVING GUARD GUIDANCE**

1. Mission: To provide periodic security checks of specified MEVA, and other designated sensitive areas/facilities within the assigned patrol areas on Fort Hood. Accurately log/record incidents observed, and report any discrepancies. Including criminal, security and/or safety which are observed during performance of military security guard duties.

2. Authority. Authority for the establishment and maintenance of the Fort Hood Military Security Guard/Patrol Program is outlined in AR 210-10 (Installation Administration), paragraph 2-9. (This regulation states: 'COMMANDERS ARE RESPONSIBLE FOR ENSURING THAT CRIMINAL ACTIVITY OR SUSPECTED CRIMINAL ACTIVITY IS REPORTED TO THE MILITARY POLICE FOR APPROPRIATE INVESTIGATION.')

3. Personnel. Military security guard force personnel will conduct themselves in a professional manner, using proper tact, military bearing and courtesy to both peers and supervisors. Height and weight will be maintained within prescribed standards.

4. Uniform/Appearance: BDU will be properly worn, and will include load bearing equipment (LBE) with poncho folded over the pistol belt and centered in the small of the back, canteen with water, first aid pouch with packet, flashlight and kevlar helmet with cover. No uniform/equipment modification is authorized unless approved by higher authority. Uniforms will be kept in a high state of police, clean and pressed, with highly shined footgear. Headgear will always be worn. The hair will be neatly trimmed and IAW military standards. Excessive jewelry, including earrings, will not be worn. Alcohol will not be consumed twelve hours prior to scheduled shift.

5. Use of Force: Military security guard force personnel may question suspicious individuals, but will not confront any suspicious person(s), vehicle(s), or situation(s) that may require use of force. In situation(s) which require MP intervention, military security guard force personnel will immediately notify the MP via radio or telephone. Guards will attempt to contain the situation or maintain surveillance. Guard will provide situation reports to the MP station pending arrival of MP personnel on the scene. Security guard force personnel are additional 'eyes and ears' for MP operations to enhance the security posture of Fort Hood, but will not engage in any type of offensive law enforcement operations unless the situation is life threatening or a threat to national security (see appendix K).

6. Duty Vehicle: Vehicles will be US Government (GSA) owned/leased of a size and type (4x4, 1/2 ton Pick-Up, sedan, etc.) required to safely and properly perform security patrol functions within the assigned patrol areas. Vehicles will be properly maintained and serviced by assigned driver(s) IAW existing regulations and standing operating procedures (SOPs).

#### 7. Patrol Area Structure:

a. Personnel: Patrol will at a minimum consist of one uniformed individual equipped with a hand held or vehicular mounted radio transmitter/receiver tuned to the appropriate BC command frequency.

b. Vehicle: Vehicle will be US Government owned/leased and of a type suited for the patrol area.

Duties: The military security guard in each patrol area is responsible for observing, checking and reporting both verbally and in writing, any occurrence of a suspicious nature within the patrol area. This includes but is not limited to damage to any property, vehicles parked in/around sensitive MEVA's and personnel acting in such a way to attract attention to themselves or personnel loitering around sensitive areas. MEVA's will be irregularly checked so a pattern is not established. MEVA checks are the primary function of the military security patrol. Security patrol personnel will exit the vehicle and physically check the security and integrity of the structure. Structures that have alarms or alarm warning signs will not be physically touched, but will be closely scrutinized as unalarmed areas. Other listed structures will be physically checked by attempting to open accessible windows and doors and checking for signs of vandalism, tampering or illegal entry. Security checks will be recorded/logged with date, time, location and any other pertinent observations. If possible, the MP security patrol will not confront or interface with any suspicious personnel/situation other than to determine identity and authority for being in the area, but will immediately report to the MP desk by radio as much information as possible (i.e. description of person, vehicle, license plate number, location, etc.) so an MP patrol/response force can be dispatched if needed. Security personnel will function as additional 'eyes and ears' of the MP to enhance both crime reduction and the physical security posture of Fort Hood without performing statutory law enforcement duties. Regardless of which patrol area assigned, security patrol personnel will always conduct themselves in a professional manner, using tact, military bearing and courtesy to both peers and supervisor. Duties that include writing and vehicle maintenance will be completed prior to release from shift.

8. Equipment: (Government Furnished)

Military security patrol personnel will use and be responsible for the following Government equipment:

- a. Vehicle
- b. Radio
- c. Uniform, (including LBE, helmet, flashlight, etc.)
- d. Binoculars (if required)

9. Optional Equipment: (Furnished at own expense)

Military security patrol personnel are authorized to use the following:

- a. Portable spotlight (plug into cigarette lighter receptacle in vehicle).  
Other optional equipment may be authorized on a case-by-case basis by the MP supervisor.
- b. No personal weapons of any type are authorized.

### **INSPECTION/SEARCH PROCEDURES - PART III THREATCON MEASURE 21 GUIDANCE**

THREATCON Measure 21: Physically inspect visitors to the unit and a percentage of their suitcases, parcels, and other containers.

Minimum actions:

- Visitors will be stopped at entrances and asked to show positive identification and state their business in the area. Unit commanders will determine the percentage of suitcases, parcels, and other containers to check based on the current threat.
- Non military/DOD personnel/dependents will sign in/out of the unit.
- A badge system may be used to monitor personnel in specific units/sensitive areas.
- Inspections leading to suspicious indicators of criminal intent will be brought to the PMO's attention immediately. MP's will provide guidance and/or response. Unit personnel will use the force necessary to detain the visitor until MP arrival.

APPENDIX N  
SITUATIONAL DEPENDENT QUESTIONS TO BE ANSWERED BY THE  
CRISIS MANAGEMENT TEAM

N-1. Civilians.

- a. When do we send civilians home or not require them to come in?
- b. Who goes home or stays home?
- c. Who decides who goes home or stays home?

N-2. How and when should on post travel be limited?

N-3. Services.

- a. At what point do clinics at Darnall limit services?
- b. Who decides?
- c. When do other service activities limit or stop services?
- d. At what point do we close child care facilities, schools, commissaries, shoppettes, clubs, etc.?

N-4. Mission Essential Personnel.

- a. Who are the mission essential key operational personnel?
- b. How do ACP personnel identify key operational personnel?
- c. How is expeditious entry provided for?

N-5. Provisions for CMT, TMF and SRT.

Who provides sustenances?

N-6. Operational Order/FRAGO with special tasking/instructions.

- a. When will the G3 task for augmentation of MP's when needed?
- b. What other critical taskings must the CMT issue? When?

## GLOSSARY

## SECTION I - ABBREVIATIONS

AC	Active Component
ACofS	Assistant Chief of Staff
ACP	access control point
ADP	automatic data processing
AG	Adjutant General
AHA	ammunition holding area
AMO	Automation Management Office
AOC	Army operation center
ASP	ammunition supply point
BC	base cluster
BASEOPS	base operation
BCC(s)	base cluster commander(s)
BDU	battle dress uniform
CofS	Chief of Staff
CAMO	Central Ammunition Management Office
CBT/T	combatting terrorism
CCTV	closed circuit television
CG	Commanding General
CI	counterintelligence
CMT	Crisis Management Team
COC	Corps operations center
COMSEC	communications security
COMCEN	communications center
CONUS	Continental United States
DA	Department of the Army
DCG	Deputy Commanding General
DCP	Directorate of Civilian Personnel
DENTAC	dental activity
DEH	Directorate of Engineering and Housing
DHS	Directorate of Health Services
DOC	Directorate of Contracting
DOD	Department of Defense
DOIM	Directorate of Information Management
DOL	Directorate of Logistics
DPCA	Directorate of Personnel and Community Activities
DPIL	Directorate of Program Integration and Leadership
DRC	Directorate of Reserve Component
DRM	Directorate of Resource Management
DSEC	Directorate of Security
EHF	emergency high frequency
EOC	Emergency Operations Center
EOD	explosive ordnance disposal
FBI	Federal Bureau of Investigation
FHIG	Fort Hood Inspector General
FRAGO	fragmentary order
FHCTP	Fort Hood Combatting Terrorism Program
FORSCOM	United States Forces Command
FOUO	For Official Use Only
FSEP	FORSCOM Security Enhancement Program
FTX	field training exercise
HAAF	Hood Army Airfield
HRP	high risk personnel
IAW	in accordance with
IDS	intrusion detection system

JCS	Joint Chiefs of Staff
LBE	load bearing equipment
MARS	military affiliated radio station
MEDDAC	medical department activities
MEVA	Mission Essential/Vulnerable Area
MI	military intelligence
MP	military police
MSC	major subordinate command
MSE	mobile subscriber equipment
NCOIC	noncommissioned officer in charge
NFH	North Fort Hood
O/O	on order
OCONUS	outside continental United States
OIC	officer in charge
OPCON	operational control
OPLAN	operation plan
OPSEC	operations security
PAO	Public Affairs Office
PCS	permanent change of station
PM	provost marshal
PMO	Provost Marshal Office
POC	point of contact
POI	program of instruction
POL	petroleum, oil and lubricants
PTM	Plans and Training Management
RGAAF	Robert Gray Army Airfield
SAEDA	Subversion and Espionage Directed Against the Army
SC	senior council
SCIF	sensitive compartmented information facility
SGS	Secretary of the General Staff
SJA	Staff Judge Advocate
SOI	signal operating instructions
SRT	special reaction team
TC/A	Terrorism Counteraction
TDY	temporary duty
TEXCOM	TRADOC Experimentation and Test Command
THREATCON	terrorist threat condition
TMF	threat management force
USACIDC	United States Army Criminal Investigation Command
USAF	United States Air Force
USAISC	United States Army Information Systems Command
USAJFKSWC	United States Army John F. Kennedy Special Warfare Command
USANG	United States Army National Guard
USAMPS	United States Army Military Police School
USAR	United States Army Reserve
VIP	very important person
WFH	West Fort Hood
WG	working group

## SECTION II - TERMS

Antiterrorism - Defensive measures used to reduce the vulnerability of personnel, family members, facilities, and equipment to terrorist acts. This includes the collection and analysis of information to accurately assess the magnitude of the threat.

**Combatting Terrorism** - (DOD) Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism) taken to oppose terrorism throughout the entire threat spectrum.

**Countering Terrorism** - Systematic measures taken during both the proactive and reactive phases of an operation to reduce terrorist incidents from occurring on military installations.

**Counterterrorism** - Offensive measures taken to respond to a terrorist act, or the documented threat of such an act, including the gathering of information and threat analysis in support of these measures.

**Crisis Management Team** - A team found at a major Army command or installation level. A CMT is concerned with plans, procedures, techniques, policies, and controls for dealing with terrorism, special threats, or other major disruptions occurring on Government installations and facilities. A CMT considers every aspect of the incident and establishes contact with the Army Operation Center (AOC).

**Force Protection** - Security program designed to protect soldiers, civilian employees, facilities, and equipment, in locations, and situations, accomplished through planned and integrated application of CBT/T, physical security, operations security, personal protective services, and supported by counterintelligence and other security programs.

**High Risk Personnel** - Personnel who, by their grade, assignment, symbolic value, location, or specific threat, are more likely to be attractive or accessible terrorist targets. Major General and above.

**Hostage** - Any person held against his or her will as security for the performance or nonperformance of specific actions.

**High Threat Area For Travel Security** - Those terrorist threatened areas identified by either the Principal Deputy Assistant Secretary of Defense for International Security Affairs (PDASD/ISA) memorandum, (subject: Travel Security), the International Threat Analysis Center (ITAC) Monthly Intelligence Summary (MITSIS) or, by the commander responsible for the area concerned.

**Major Disruptions on Installations, Units, and Facilities** - Acts, threat, or attempts to commit such acts as kidnapping, extortion, bombings, hijackings, ambushing, major weapons thefts, arson, assassination, and hostage taking on a military installation, unit, or facility. Acts that have potential for widespread publicity require special response, tactics, and management.

**Mission Essential/Vulnerable Areas** - Facilities or activities within the installation that, by virtue of their function, are evaluated by the commander as vital to the successful accomplishment of the installation's mission. This includes areas nonessential to the installation's operational mission but which, by nature of the activity, are considered vulnerable to theft, trespass, damage, or other criminal activity.

**Negotiations** - A dialogue between authorities and offenders that has, as the ultimate goal, the safe release of hostages and the surrender of the offenders.

**Primary Targets** - Targets of high publicity value to terrorists.

**Proactive** - Measures in the preventive stage of antiterrorism which include actions such as planning and training, designed to harden targets and detect a planned action before it occurs.

**Reactive** - The command's response to an ongoing terrorist incident. Success of the reactive measures is largely dependent upon the planning and training conducted during the proactive stage. The reactive stage includes activation of the EOC, deployment of the special reaction team, etc.

**Secondary Targets** - Targets of lower publicity value, used as alternates when the primary target is unattainable.

**Special Reaction Team** - A specially trained team of military/security personnel serving as the installation commander's principal response force in the event of a major disruption of threat situation on the installation. The SRT is armed and equipped to isolate, contain, gather information for, and if necessary, neutralize a special threat. Mission employment of the SRT may include resolving barricaded criminal situations; resolving sniper situations; rescuing hostages; apprehending suspects; and collecting and reporting intelligence during special threat situations.

**Special Threat** - Any situation involving a sniper, barricaded criminal, hostage taker, or any terrorist incident that requires special response/reaction, manpower management, training, and equipment.

**Threat Analysis** - Analyzing an installation's vulnerabilities to a terrorist threat to help uncover and isolate security weaknesses.

**Threat Management Force** - An action force from the installation that responds to major disruptions on an installation. The TMF will be of sufficient size to manage the disruption and will usually involve a command element, security element, negotiation team, SRT, and logistical element.

**Terrorism** - The calculated use of violence or the threat of violence to attain goals, political, religious, or ideological in nature. This is done through intimidation, coercion, or instilling fear. Terrorism involves a criminal act that is often symbolic in nature and intended to influence an audience beyond the immediate victims.

**Terrorist Group** - A politically, religious, or ideologically oriented group that uses terrorism as its prime mode of operations."