FORT HOOD

Army Internal Review Team: Final Report

Protecting our Army community
at home & abroad

Report Date | August 4, 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
04 AUG 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Fort Hood Army Internal Review Team: Final Report	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Secretary of the Army,Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

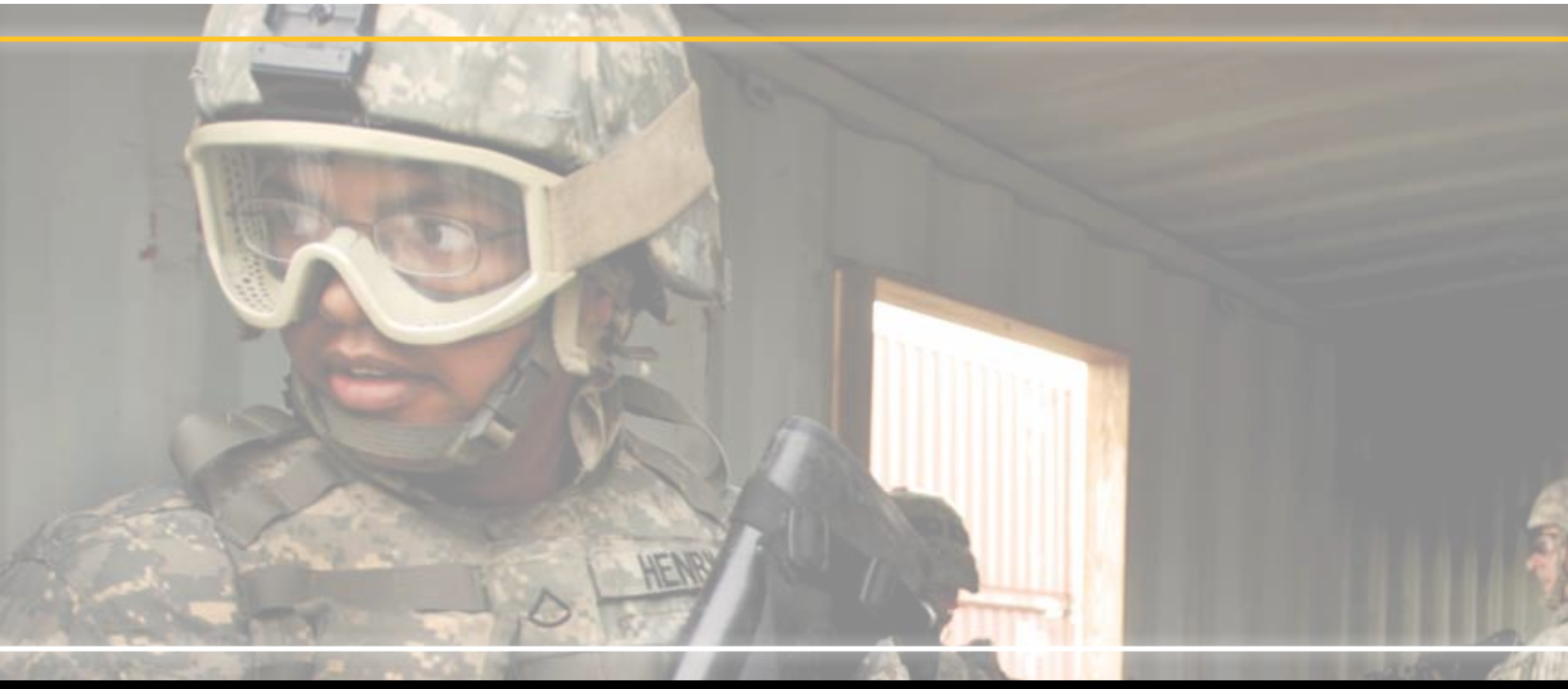
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**122**	



SECRETARY OF THE ARMY
WASHINGTON

AUG 16 2010

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (HOMELAND DEFENSE AND AMERICA'S SECURITY AFFAIRS)

SUBJECT: Fort Hood Army Follow-On Internal Review Final Report

By memorandum of 29 January 2010, subject: *Follow-on Action on the Findings and Recommendations of the DoD independent Review Related to the Fort Hood Incident*, the Secretary of Defense tasked the Secretaries of the Military Departments, Combatant Commanders and the heads of the other Department of Defense (DoD) components to initiate internal reviews to assess each organization's ability, below the headquarters level, to identify internal threats and force protection and emergency response programs, policies and procedures. Enclosed please find the report of the Army's internal review.

In addition to conducting our internal review, the Army is rapidly moving forward to implement the recommendations of the DoD Independent Review Panel—thus far we have implemented 21 of the 79 DoD Independent Review Panel recommendations and have initiated action to implement 45 additional recommendations. The remaining thirteen recommendations require DoD action prior to Army implementation. The Army's internal review identified several initiatives not addressed in the DoD Independent Review Panel Report. These initiatives and their proposed implementation are detailed in our final report.

The Army will continue to work closely with DoD, the Combatant Commands, and the other Services to improve the protection of our people and facilities across the Department.

John M. McHugh

Encls

This page has been left blank intentionally

FORT HOOD

ARMY INTERNAL REVIEW TEAM: FINAL REPORT

EXECUTIVE SUMMARY

Overview

The Army's Soldiers, Families and Civilians deserve a safe and secure environment to work, train and live. The Army's efforts in this regard are not new and they began long before the tragic events of 5 November 2009 at Fort Hood, Texas where the Army family lost thirteen of its members and 31 wounded. The Fort Hood Army Internal Review Team dedicates the recommendations and plans in this report to the victims and their families with the prospect of precluding such an event from happening in the future.

FORT HOOD'S USE OF AN ACTIVE SHOOTER RESPONSE MODEL SAVED LIVES . . . prior mass casualty management and training, investment in emergency equipment and coordination with civilian law enforcement and emergency response personnel made a difference.

As the Department of Defense (DoD) Independent Review Panel made clear in its report, "the initial response to the incident was prompt and effective." Fort Hood's use of an Active Shooter Response (ASR) model saved lives. Without question, prior mass casualty management and training, investment in emergency equipment and coordination with civilian law enforcement and emergency response personnel made a difference. Still, the DoD Independent Review Panel identified 79 recommendations for consideration and/or implementation DoD-wide to reduce the likelihood, react to and recover from future incidents. While much has been accomplished, we believe that more can be done.

Subsequent to the publication of the DoD Independent Review Panel's report, the Secretary of Defense directed the Services to report back to the Assistant Secretary of Defense for Homeland Security and Americas' Security Affairs (ASD(HD&ASA)), the Services internal review and assessment of "their organization's ability below the headquarters level to identify internal threats and force protection (FP) and emergency response programs, policies and procedures." In response to the Secretary of Defense's directive, the Army Vice Chief of Staff (VCSA) established the Fort Hood Army Internal Review Team (AIRT). The result of the Internal Review Team's effort is this report.

Army Installation Assessment and Best Practices

The focus of the Army effort is to provide installation commanders the tools they need to support the senior commander's mission to protect the force. To that end, the Installation Management Command (IMCOM) Commander identified the following functions as critical to mission accomplishment:

1. All installations must have an Emergency Operations Center (EOC) that is fully capable.
2. All installation staffs understand the reporting chain is through the senior commander, simultaneously to the Army Operations Center and the respective Army Service Component Command (ASCC); ASCCs report to their Combatant Commander.
3. Installations maintain current and comprehensive agreements with key emergency responders in the local community (law enforcement, fire, medical, etc.).
4. Installation staffs must exercise 1 through 3 above frequently.

THE DEMANDS of internal and external threats require us to sharpen our focus.

In response to the DoD directive to review and assess the Army's ability below the headquarters level to identify internal threats and FP and emergency response programs, policies and procedures the Fort Hood AIRT: visited 17 installations; conducted a data call from Army Commands (ACOMs), Direct Reporting Units (DRUs) and the Army National Guard; and surveyed over 80 installation commanders. The installation commanders emphasized the need for funding and personnel to meet additional protection requirements, the demands that result from implementation of the DoD findings and recommendations and the need to sustain existing equipment. The Army focus is on providing installation commanders the tools they need to support the senior commander's FP mission. However, the demands of internal and external threats require us to sharpen our focus. To meet these mission critical tasks, the Army must evolve and transform.

Our 17 site visits highlighted an important point: the Army is not homogenously-based. Incident reporting practices overseas and incident reporting in the Continental United States (CONUS), coupled with Joint Basing, lead to varied reporting practices. As Fort Hood demonstrated, communication is critical to timely response. ACOMs share concern for prompt, uniform and comprehensive reporting procedures. Installation commanders said they were hampered in their reporting efforts by multiple reporting chains and report formats. In our report, we recommend the Army G-3/5/7 (G-3/5/7) publish incident reporting procedures from installation level to Headquarters, Department of the Army (HQDA).

The Army was well along a path of change prior to and immediately following the Fort Hood incident. Many initiatives were already in progress to mitigate the insider threat. IMCOM published a campaign plan. Medical Command (MEDCOM) installations will transfer to IMCOM control by the end of fiscal year (FY) 2011. Army Materiel Command (AMC) and IMCOM are using four installations to conduct a pilot to determine how to transfer AMC special installations to IMCOM control. The Comprehensive Soldier Fitness (CSF) program represents the Army's investment in readiness of the force and quality of life for our Soldiers, Family members and Civilians. The goal of CSF is to increase resilience and enhance performance by developing the five dimensions of strength: physical, emotional, social, spiritual and family. In order to increase resilience in health care providers, the Army Office of the Surgeon General (OTSG)/MEDCOM initiated the Care Provider Support Training program, and others, with additional emphasis for behavioral health providers. All of these

efforts were on-going prior to 5 November 2009. Immediately following the Fort Hood incident, the Army Chief of Staff established the Insider Threat Task Force on 16 November 2010, led by the Army G-2 (G-2) and IMCOM Commander that has produced distinctive results in the areas of counterintelligence (CI) and security.

Our "deep dive" identified best practices that warrant consideration for adoption across the force: FP assessments of all ACOMs, DRUs and ASCCs by the G-3/5/7 once every three years; the CSF directorate and program; civil support team training; comprehensive and current memoranda of understanding between installations and local emergency response capabilities; cooperative annual emergency response training with local authorities; empowering supervisors as case managers in employee injury and death cases; partnering with industry in no-cost relationships to provide state of the art technology; FP compliance worksheets; situational intelligence reports for special events; designated Family Assistance Center (FAC) Teams; computer back-up programs; and using emergency operation equipment that is interoperable with that of local authorities and responders.

DoD Independent Review Panel Report Major Areas

The Army is moving forward on the recommendations contained in the DoD Independent Review Panel Report. The DoD report focused on five major areas: Personnel, FP, Information Sharing, Installation Emergency Response and Health Affairs. Of the 79 recommendations, the Army has implemented 21 of them and is in varying stages of implementing or partially implementing 45 recommendations pending DoD guidance/policy. The remaining 13 recommendations require DoD policy updates and/or revisions in order for the Army to commence implementation.

IN GENERAL the Army has sufficient personnel policy guidance for implementing personnel support programs and services.

In our Personnel review, we found in general the Army has sufficient personnel policy guidance for implementing personnel support programs and services. In some cases, however, personnel policy guidance and programs address unique requirements such as mass casualty, crisis incidents, workplace violence and religious accommodation. To address these update requirements, the Army will provide interim guidance while awaiting development and release of formal DoD policy. The Army G1 and Office of the Chief of Chaplains (OCCH) will lead these efforts through work with Under Secretary of Defense (Personnel & Readiness) USD(P&R) and the Armed Forces Chaplains Board.

For FP, the Army developed a draft implementation plan for the recommendations in this major area pending receipt of DoD guidance. In our internal review, the Army found that we possess sufficient policy guidance for implementing protection programs, but lack a synchronizing organization or synchronizing function within an existing organization. In most cases, FP policy guidance and programs require updates and/or actions to address unique requirements such as behavioral indicators, real time information sharing, integrated FP policies, internal threats, screening strategies and capabilities. As an example, HQDA conducts protection assessments of each ACOM, ASCC and DRUs once every three years by identifying trends and problem areas. If regulatory gaps are discovered, that information drives changes to Army policies.

The synopsis of the findings and recommendations in the Information Sharing area was the lack of policy, procedures and systems for the sharing of threat related information between the Services, Combatant Commands, DoD and other federal agencies such as the Federal Bureau of Investigation (FBI). The inadequacy of information sharing between critical components of DoD's FP enterprise

was the common thread between each of the four findings and seven recommendations in this area. The Army helped to develop the initial policies being drafted by DoD to improve information sharing and will continue this effort until the policies are published. The Army also is working to address the internal information sharing issues found by the AIRT during the visits to specific Army installations.

The Army identified and analyzed the Installation Emergency Response issues and is establishing working groups to further address areas of concern. The Army established Emergency Management (EM) as a formal program of record with the release of Army Regulation (AR) 525-27, *Army Emergency Management Program*. Department of Defense Instruction (DoDI) 6055.17 directs the Services to achieve Initial Operational Capability (IOC) no later than 13 January 2011 and Full Operational Capability (FOC) no later than 13 January 2014. IOC requirements focus on initial actions to field and utilize Installation Emergency Managers at all DoD Installations responsible for developing and executing the Installation Emergency Management (IEM) Program across all five phases of the emergency lifecycle: Preparedness, Mitigation, Prevention, Response and Recovery. FOC targets are a multi-year effort requiring the organization, manning, training, equipping and exercising of multiple capabilities across the EM lifecycle addressing all hazards.

To attain FOC, the Army is establishing working groups, led by the G-3/5/7, to determine standards, requirements, baseline current systems and developed a plan for acquisition, fielding and sustainment to close identified gaps for implementing the following initiatives: an enhanced 911 (E911) system; a Mass Warning and Notification (MWN) system enabling commands to quickly and effectively warn the installation of emergencies and direct protective actions before, during and after an incident; and a Common Operating Picture (COP) capability enabling commands to quickly and effectively exchange information resource requests and coordinate response and recovery operations with civil and military partners.

THE ARMY CONDUCTED EXTENSIVE RESEARCH and incorporated federal, state, and local law enforcement best practices into the training curriculum, including Active Shooter Response (ASR), for Army Civilian Police, Security Guards, and Military Police.

Additionally, the impact of the Fort Hood Shooting displayed the need for DoD to establish preventive measures as well as identify enhanced methods for emergency response personnel. The Army conducted extensive research and incorporated federal, state and local law enforcement best practices into the training curriculum, including ASR, for Army Civilian Police, Security Guards and Military Police (MPs). The U.S. Army Military Police School (USAMPS) developed an ASR Training Support Package (TSP) in March 2010 for Army Civilian Police and MPs.

In Health Affairs, the Army found that it possesses sufficient policy guidance for implementing medical care to include policies that appropriately addressed behavioral health conditions. The Army's OTSG and MEDCOM developed the Comprehensive Behavior Health System of Care Campaign Plan for incorporation into the Army Campaign Plan. Its purpose is to clearly delineate existing policies, procedures and guidance to establish minimum standards for Traumatic Event Management (TEM), Soldier and Health Care Provider support.

Quick Wins

The Army began taking action to improve EM before and since publication of the DoD Independent Review Panel's report. Prior to the publication of this report, the Army implemented 10 "quick wins."

1. In an active shooter scenario, the response is action, not cordon; the Office of the Provost Marshal General (OPMG) and the USAMPS, with the assistance of the G-3/5/7, now trains all military and civilian law enforcement to respond with proven tactics.

2. MPs are now authorized to use jacketed hollow point ammunition to reduce the risk of injury to innocent bystanders.

3. The General Officer Management Office revised General Officer assignment orders to expressly reflect senior commander authorities, responsibilities and duties.

4. General Officers selected as a senior commander are required to attend the General Officer/Senior Commander Course at the Army Management Staff College and are trained on the Army's EM program to improve their understanding prior to an actual emergency.

5. In order to identify internal and external threats to Army personnel, the G-2 initiated a rapid revision and re-titled AR 381-12, formerly Subversion and Espionage Directed Against the Army (SAEDA), now Threat Awareness and Reporting to include additional observable indicators for espionage, terrorism and extremism. The AR has completed legal review and is waiting for approval from the Army Publishing Directorate.

6. The Army developed and implemented the iSalute CI reporting system via "Army Knowledge Online" and "Army Knowledge Online – Secure" internet based reporting links in April 2010. The G-2 and Chief Information Officer/G-6 developed and implemented the reporting platforms enabling any Soldier or civilian with an Army Knowledge Online or Army Knowledge Online – Secure account to report a suspicious activity to Army CI.

7. The Army's new iWATCH program promotes anti-terrorism across all commands and leverages every member of the Army community as a sensor with reporting at the local level.

8. As a new paradigm for dealing with trauma regardless of origin, the Army implemented the TEM Course at the Army Medical Department (AMEDD) Center and School. This course trains behavioral health providers, related healthcare professionals and Unit Ministry Teams in traumatic event management and standardizes how the Army will provide trauma management.

9. The Army Surgeon General and MEDCOM implemented Care Provider Support training to teach healthcare providers how to manage stressors unique to providing health care.

10. The United States Army Crime Center, in concert with the FBI Criminal Justice Information System (CJIS), amended the CJIS Security Policy authorizing contract security guards (CSGs) access to the National Crime Information Center (NCIC). This change enables installations without law enforcement personnel the ability to conduct criminal checks on civilians attempting to enter the installation.

The above demonstrates that the Army can quickly adapt, but there are enduring FP challenges that require discipline. The Army must address a number of important initiatives in our standard management forums: Force Structure Panel, concept plan approval process, the Budget Requirements and Programming (BRP) board process and establish decision points in the Army Campaign Plan.

Emerging Ideas

There are a number of initiatives the Army must implement in order to address systemic challenges with our current procedures to protect the force. In order to move forward, the Army must address these issues in our standard management forums, such as our force structure validation process

documented by the concept plan approval process and our BRP, all tracked by establishing decision points in the Army Campaign Plan.

OUR CURRENT PROTECTION PROCEDURES FALL SHORT of synchronizing policy, establishing priorities and allocating resources to achieve the desired end state

Our current protection procedures fall short of synchronizing policy, establishing priorities and allocating resources to achieve the desired end state. The Army senior leadership is not given the opportunity to affect the end state because they cannot review the portfolio of protection related functions on a recurring basis.

The Army must implement goals and objectives as directed by the Secretary of the Army in his directive on Army Protection in April 2008. In this directive Secretary Geren clearly designated the G-3/5/7 as the staff agent responsible for Army Protection Policy. Implementing this directive corrects shortfalls in how we implement policy, prioritize requirements and program necessary resources to meet current and emerging protection requirements at our installations. Our current process does not synchronize all Army protection-related functions into a coherent program to maximize security providing unity of effort. As an example within the EM function, we will likely fail to meet National Incident Management System (NIMS) IOC and FOC mandated milestones, unless we transform how the Army manages this program.

Additionally, the Army must adapt to procedures put in place since Secretary Geren signed Army Directive 2008-02. ACSIM has proposed changes to the 2011 Army Campaign Plan that identifies "Provide a Safe & Secure Working & Living Environment" as Major Objective 2-7 which is nested in Campaign Objective "Provide an Effective Protection Capability at Army Installations" (see Appendix G). The Army should designate the G-3/5/7 lead for Major Objective 2-7 as part of the Army Campaign Plan process.

Currently, installation commanders identify and prioritize EM equipment they need. Equipment is not direct funded, procured locally and must compete for sustainment. We recommend that the Secretary of the Army direct the establishment of an Army funding line for centralized management of the equipment and the Army Acquisition Executive appoint a Program Manager(s) with resources and authority for life cycle management of EM equipment. The Army must designate this equipment as "programs of record" and program the funding necessary to achieve both IOC and FOC as outlined in current DoDI and the NIMS and National Response Framework (NRF).

The team found the legal authority of CSGs to respond to an active shooter threat is unclear. The lack of clarity is exacerbated by the multiple types of jurisdictions on our installations: exclusive (Federal), proprietary (State), or concurrent. Over the past nine years, the Army has relied heavily on CSGs. This is changing. IMCOM is actively converting its 1,679 CSGs to Department of the Army Security Guards (DASGs) and will complete force revisions by the end of FY 2010. In the years since 9/11, the Department and Service Secretaries contracted for increased performance of security guard functions on the authority provided in periodic annual National Defense Authorization Acts. In this era, the Army must anticipate "in-sourcing" and consider how to bridge FP requirements with available resources.

The effort to convert CSGs to DASGs did not extend to non-IMCOM installations and there is confusion associated with their capability, authority and risk associated with their use. Currently, AMC has 540 CSGs and the United States Army Corps of Engineers has 79. We need to ensure that we can respond effectively to an active shooter scenario, especially at Army installations without a

installation commander ("non-traditional/separate facilities"). We also need to ensure that CSGs receive training on the new active shooter scenario across the Army. The Army must definitively establish the limitations of authorities for CSGs given the various jurisdictions in which we operate. We recommend that OPMG lead a cost-benefit-risk analysis to determine the best means for FP and security at all installations, including non-traditional/separate facilities. The Army must use this analysis to establish clear policy and procedures regarding the authority and actions of CSGs in response to an active shooter and a standard equipping package for all Army security personnel.

Several initiatives will affect force structure of the garrison staff. As an example, the Army concurred with DoD's recommendation to use the FBI's e-Guardian System reporting suspicious activity. This action will result in an increase in personnel and equipment requirements across the Army. Another example is where installation commanders reported that they did not have the resources to adequately conduct installation threat analysis and that they do not receive necessary levels

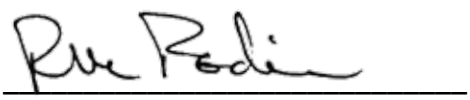
WE recommend The Army develop an installation staff Battle Command Training Program

of external support for threat analysis. Consequently, the G-2, G-3/5/7 and OPMG are working to develop a strategic information sharing concept to provide timely information, allowing installation commanders access to critical information aimed at protecting their force. This concept plan uses a combination of information sharing technology and personnel to ensure robust information sharing that should be presented to the ASA(I&E), then forwarded to the G-3/5/7 for validation. We recommend the Army develop an installation staff Battle Command Training Program which could result in increased resource requirements for both the installation and US Army Training and Doctrine Command (TRADOC). Lastly, to enable IOC and FOC for IEM, the Army will require trained and certified EM professionals.

Summary

We must efficiently and effectively transform how we look at protecting the force. Many of the DoD Independent Review Panel recommendations and the emerging ideas developed by the Fort Hood AIRT require further staffing and policy review for a complete solution. The Army must ensure that an enterprise approach is used to further develop our recommendations and emerging ideas. The approach must using existing forums, such as the SICE Board, to fully vet and present to the Army Senior Leadership for decision as part of the Army Campaign Plan. As part of the vetting process, the Army must also take this opportunity to explore other

Services' solutions and collaborate with the Office of the Secretary of Defense (OSD) to ensure success against our Nation's internal, external and asymmetric threats.



Robert M. Radin
Major General, U.S. Army
Army Internal Review Team Leader

Table of Contents

Chapter 1. INTRODUCTION

A. Background.

On 5 November 2009, a gunman opened fire on military and civilian personnel at the Soldier Readiness Center at Fort Hood, Texas. Thirteen people were killed and 43 others were wounded, 34 by gunshot and 9 by other means. While the response to the incident was prompt and effective, the tragedy raised questions about the DoD's preparedness to prevent or defend against internal threats. Immediately following the shooting, Defense Secretary Robert M. Gates established the DoD Independent Review Panel headed by the Honorable Togo West and Admiral Vernon Clark. In January 2010, the DoD Independent Review Panel published its report setting forth seventy-nine recommendations, divided into five major areas: personnel, information sharing, force protection, installation emergency response and health affairs.

On 29 January 2010, in a memorandum entitled, "Follow-on Action on the Findings and Recommendations of the DoD Independent Review Related to the Fort Hood Incident," the Secretary of Defense directed the DoD and each Military Department to initiate internal reviews based on the report of the DoD Independent Review Panel.

The Secretary of the Army established the Fort Hood AIRT in response to this directive. On 1 March 2010, the VCSA appointed MG Robert Radin to lead the Fort Hood AIRT. The Fort Hood AIRT is composed of representatives from the following HQDA staff agencies:

- Assistant Secretary of the Army (Manpower & Reserve Affairs) (ASA(M&RA))
- Deputy Chief of Staff, G-2
- Deputy Chief of Staff , G-3/5/7
- Assistant Chief of Staff, Installation Management (ACSIM)
- Office of the Surgeon General
- Deputy Chief of Staff, G- 8, Center for Army Analysis (CAA)
- Office of the General Counsel (OGC)/Office of the Judge Advocate General (OTJAG)
- Office of the Provost Marshal General

The below HQDA staff agencies provided associate team members:

- Office of the Chief of Chaplains
- Office of the Chief Information Officer/G-6 (CIO/G-6)
- Office of the Chief of Legislative Liaison
- Army Audit Agency (AAA)
- Assistant Secretary of the Army (Financial Management and Comptroller)(ASA(FM&C))
- Office of the Chief of Public Affairs (OCPA)

B. Mission.

On 19 April 2010, General Peter W. Chiarelli, VCSA, tasked the Fort Hood AIRT with the following mission:

- Assess the Army's ability below the headquarters level to identify internal threats, FP and emergency response programs, policies and procedures and prepare a draft report of the team's findings for submission to the ASD(HD&ASA).
- Develop an action plan, for Senior Army Leader approval, to implement those findings and recommendations of the DoD Independent Review Panel Related to Fort Hood ultimately approved by the Secretary of Defense.
- Develop recommendations and corresponding implementation plans for any actions not recommended by the DoD Independent Review Panel that the Fort Hood AIRT determines will facilitate the Army's ability to improve identification of internal threats, FP, or emergency response capabilities.

C. Charter.

After reviewing the Secretary of the Army's intent and the Independent Review Panel's findings and recommendations, the Fort Hood AIRT established a Charter, signed by the VCSA, with the following objectives:

- Coordinate and obtain data from Army installations to assess the Army's ability below the headquarters level to identify internal threats, FP and emergency response programs, policies and procedures.
- Prepare a draft report for submission to the ASD(HD&ASA) assessing the Army's programs, policies and procedures for the identification of internal threats, FP and emergency response.
- Act as the Army lead for coordination with the OSD staff involving the Services' follow-on review of the DoD Independent Review Panel's findings and recommendations.
- Conduct a comprehensive review of the DoD Independent Review Panel findings and recommendations and develop an implementation plan for those recommendations approved by the Secretary of Defense.
- Critically evaluate whether there are any other actions that will facilitate the Army's ability to improve identification of internal threats, FP, or emergency response capabilities and develop recommendations and an implementation action plan for Senior Army Leadership approval.
- Work collaboratively with other Services' subject matter experts (SMEs) and Federal agencies to determine and implement the best practices and solutions in each of the five topic areas: personnel, information sharing, FP, installation emergency response and health affairs.
- Identify immediate and enduring Army policy and doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) solutions that will enable the Army's efforts to prevent similar incidents from occurring.
- Identify immediate and enduring HQDA policy and DOTMLPF solutions that will assist the Army to more effectively react to a similar future incident should it occur.

D. Fort Hood Best Practices.

From the outset, III Corps and Fort Hood, the Independent Review Panel and the Fort Hood AIRT identified Fort Hood's actions that constitute "best practices" to be instituted throughout the Army. The Fort Hood AIRT identified seven best practices in review of the DoD Independent Review Panel and the III Corps and Fort Hood after action reports:

- Timely Response. The DoD Independent Review Panel determined that the "initial response was prompt and effective." Installation responders arrived on scene in two minutes and forty seconds and incapacitated the alleged perpetrator within four minutes and ten seconds after the 911 call. Fort Hood's anticipation of mass casualty events and emergency

...THE 1ST RESPONSE LAW ENFORCEMENT TECHNIQUE of "taking the fight to the shooter versus creating a cordon and awaiting SWAT type forces" saved lives

response plans and "the prompt and courageous acts of Soldiers, first responders, local law enforcement personnel, DoD civilians and healthcare providers prevented greater losses."

- III Corps and Fort Hood conducted an after-action review. They concluded that the 1st Response Law Enforcement technique of "taking the fight to the shooter versus creating a cordon and awaiting SWAT type forces" saved lives. III Corps and Fort Hood recommended that this training be mandated Army wide.
- III Corps and Fort Hood concluded that use of the Big (Giant) Voice to advise the Post of the situation and issue instruction worked well to inform of basic information.
- Plan for, identify and exercise a Crisis Response Battalion (CRB) for FP at installations where such units are available. The CRB was used for cordoning the crime scene, augmenting access control points and effectively executed enhanced FP condition measures at 22 sites on Fort Hood.
- A dedicated Provost Marshal (PM) cell facilitated MP functions throughout the event. This is in addition to the MP Brigade Commander, who was deployed during the event. The dedicated PM cell facilitated the coordination of law enforcement and criminal investigative efforts and ensured vertical information flow to the command group.
- Multi-agency first responder cooperation was outstanding due to the excellent relationship building efforts by Fort Hood emergency response personnel and a multitude of civilian agencies that monitor the emergency net and responded without official requests from Fort Hood. The habitual and enduring relationship enabled the agencies to take direction from the Fort Hood mobile emergency command post to ensure unity of effort and command on scene.
- mmediate trauma and grief counseling was provided by Fort Hood through Chaplains on site and counseling provided within 72 hours of the incident. Behavioral health specialists were set up on site and facilitated recovery for employees and military personnel.

Chapter 2. ASSESSMENT OF ARMY INSTALLATIONS

A. Background.

The Secretary of Defense directed the Services to assess their ability below the headquarters level to identify internal threats, FP and emergency response programs, policies and procedures. Subsequently, the VCSA established the Fort Hood AIRT to conduct the assessment. As part of the internal review and assessment, the AIRT determined that it was in the Army's best interests to identify immediate and enduring Army policy and DOTMLPF solutions that will enable the Army effort to preclude, respond and recover from an incident similar to the Fort Hood shooting.

...TEAMS MET WITH SENIOR MISSION COMMANDERS, installation commanders and key staff elements and conducted detailed interdisciplinary discussions.

Major General Robert Radin was appointed to lead an assessment team consisting of eleven full-time members and seven SMEs selected from positions within the HQDA Staff to conduct installation visits as part of the assessment. Members of the installation assessment team were:

- Major General Robert Radin, AIRT Leader
- Colonel Allen Kiefer, AIRT Chief of Staff
- Colonel Kerk Brown, ASA(M&RA) Lead
- Colonel Jimmy Daniels, OTSG/MEDCOM Lead
- Colonel John Domenech, G-3/5/7 Installation Emergency Response Lead
- Colonel Regina Grant, ACSIM Lead
- Colonel Micheal Hoyt, OCCH
- Colonel James Stuteville, G-2/Information Sharing Lead
- Colonel BJ Constantine, ASA(M&RA) Lead
- Lieutenant Colonel Bruce Barker, OPMG Lead
- Major Walter Dana Venneman, Legal Counsel
- Mr. Steve Birdsall, Subject Matter Expert, IMCOM
- Mr. Harvey Clark, Subject Matter Expert, IMCOM
- Mr. Sid Crews, Subject Matter Expert, IMCOM
- Mr. Jeffrey Davis, Subject Matter Expert, IMCOM
- Mr. Timothy Goff, Subject Matter Expert, IMCOM
- Mr. James Platt, Subject Matter Expert, Deputy Chief of Staff, G-3/5/7
- Mr. James Smith, Subject Matter Expert, IMCOM

B. Method for Gathering Data.

The Fort Hood AIRT organized small inter-disciplinary teams of senior officers and sent them on coordinated visits to 17 garrison commands throughout the CONUS and overseas examining identification of internal threat DOTMLPF issues. These teams met with senior mission commanders, installation commanders and key staff elements and conducted detailed interdisciplinary discussions. The team oriented the visits to include a representative sample of the types of Army Installations including: IMCOM, National Guard and AMC installations. These commands nominated the installations visited by the Fort Hood AIRT.

The Fort Hood AIRT visited the following installations:

- United States Army Garrison (USAG), Fort Bliss, Texas
- USAG, Fort Gordon, Georgia
- USAG, Fort Leonard Wood, Missouri
- USAG, Fort Stewart, Georgia
- USAG, Joint Base Lewis-McChord, Fort Lewis, Washington
- USAG, Camp Zama, Japan
- USAG, Yongsan, Korea
- USAG, White Sands Missile Range, New Mexico
- USAG, Red River Army Depot, Texas
- USAG, Watervliet Arsenal, New York
- USAG, Kaiserslautern, Germany
- USAG, Vicenza, Italy
- Nevada Army National Guard, Joint Force Headquarters
- Florida Army National Guard, Joint Force Headquarters
- Holston Army Ammunition Plant, Holston, Tennessee
- Joint Systems Manufacturing Center, Lima, Ohio
- Radford Army Ammunition Plant, Radford, Virginia

The teams met with over 300 military and civilian leaders, primary protection and EM personnel and assessed their knowledge and perceptions about the Independent Review Panel findings and recommendations. The teams also sought input into other areas in which the Army can make improvements. The assessment teams reviewed applicable DoD, Army, command and local installation directives, regulations, policies, plans, guidance, standing operating procedures and other related documents on protection and EM. The teams conducted program, policy and procedure reviews in the following areas: command and control (C2), reporting, EM, FP, identifying internal threats and actions supporting early identification, mitigation and response, EOC function, C2 Exercises, Mutual Aid Agreements (MAAs), emergency mass notification equipment and its sustainment, FAC operations, health affairs, best practices and perceived gaps.

In addition to the installation site visits, the VCSA's Fort Hood Army Follow-On Internal Review Team Tasking Memo of 19 April 2010 (See Appendix C) directed a data call to the "twenty-three DRUs, ASCCs and ACOMs to determine the usefulness and utility of programs, policies and procedures relating to FP, EM, reporting and C2.

The data call requested information to the following questions:

- Do ARs 381-12 "Subversion and Espionage Directed Against the Army (SAEDA)" and 25-2 "Information Assurance", ALARACT message 231715ZNOV09 and Joint Publication 2.0 "Joint Intelligence" help you identify internal threats? If not, why not? Are there gaps in these regulations or messages that need addressing? If so, what are they?
- Do ARs 525-13 "Antiterrorism," 190-56 "The Army Civilian Police and Security Guard Program," 190-11 "Physical Security of Arms, Ammunition and Explosives," 190-58 "Personal Security," and 190-12 "Military Working Dog Program," help you provide FP? If not, why not? Are there gaps in these regulations that need to be addressed? If so, what are they?
- Does AR 525-27 "Army Emergency Management Program" help you provide for an EM program? If not, why not? Are there gaps that need to be addressed? If so, what are they?
- Do installations understand the regulatory reporting requirements (horizontally and vertically) in the case of an internal threat, FP, or EM event? If not, what changes would make them clearer?
- Do installations understand and are the C2 relationships clear in the case of an internal threat, FP, or EM event? If not, what changes would make them clearer?
- Describe any local policies or practices that your installation would use in the case of an internal threat, FP, or EM event that you believe other installations could adopt and benefit from.

C. Surveys.

The Fort Hood AIRT forwarded digital surveys to approximately 105 installation and installation commanders with the 79 findings and recommendations. The survey required detailed review of the DoD Independent Review Panel findings and recommendations, rating each for the impact of implementation on a scale of one (least impact) to ten (most impact) and provided an opportunity for detailed comment on individual findings and recommendations (See Appendix H). The team solicited responses from 105 installation commanders and received responses from 84 installation commanders representing an 80% response rate.

Installation commanders rated the below DoD Independent Review Panel report recommendations as having high impact on their ability to conduct protection operations. See appendix D for details on each recommendation:

1. Installation level emergency operations center common operational picture. (4.5.A)
2. Leverage civilian law enforcement best practices for police and security guards. (4.3.A)
3. Automate government agency information for installation access control. (3.9.A,B,C)
4. Facilitate mass warning and notification systems. (4.4.A)
5. Establish a consolidated law enforcement database. (2.10.A)
6. Improve background checks for DoD work force. (2.2.A)

7. Active shooter and standard law enforcement training for all police (military and civilian). (4.3.B,C)

8. Combatant Commanders ensure an unclassified means to notify their installations of a Force Protection Condition change. (3.6.A)

D. In-Progress Reviews.

MG Radin conducted multiple detailed in-progress reviews with the Secretary of the Army, Army Chief of Staff and the VCSA in order to establish priorities, examine trends and progress and to receive updated guidance regarding the efforts of the team.

E. Standards Used in the Assessment.

The Fort Hood AIRT applied generally accepted government assessment standards. The team obtained sufficient and appropriate information responsive to our Charter and formed a reasonable basis for our observations.

THE ARMY HAS APPLIED A BOTTOM UP APPROACH to EM and consequently, installation EM is unlinked between installations and lacks a single staff proponent.

F. Assessment.

In general, based on responses to the data call and the team's installation visits, the Army continues improving its ability to identify internal threats, conduct FP and respond to emergencies. Multiple initiatives at multiple levels (HQDA, IMCOM and local) have been implemented or are well on their way to implementation to continue to improve the Army's posture in these areas. Due to the unique character of Army installations, a standardized solution in all areas is not necessarily a viable alternative. Installation solutions need to be threat/situation based to offer the most effective and efficient solutions. The Army has applied a bottom up approach to EM and consequently, installation EM is unlinked between installations and lacks a single staff proponent.

United States Army North (ARNORTH) asked CONUS based units of IMCOM, AMC, TRADOC and MEDCOM to provide input. ARNORTH considers those installations with an identified installation commander as "traditional installations." Those installations/separate facilities with no identified installation commander are "non-traditional/separate facilities." ARNORTH analyzed the data call and reports and found:

- IMCOM:
  - The leadership of eighty-five percent of the installations are satisfied with existing regulations, policies and procedures for identifying insider threats.
  - Confident they can execute EM and FP programs.
  - Clear on reporting requirements.
  - Clear on the C2 relationships for exercising authority and responsibility for internal threats, FP and all hazard events.

- Recommends installations conduct semi-annual training for Crisis Action Team responses and attend basic Federal Emergency Management Agency courses for certification.

- MEDCOM collected input from two installations. MEDCOM identified the below concerns:
  - Insider threat identification.
  - Unclear on reporting requirements.
  - Issues with C2 authorities during Fort Hood-type events.
  - Recommends adopting a mass notification system for installations.
- AMC and TRADOC shared similar concerns for non-traditional installations/separate facilities. Both addressed inadequate support for insider threat identification, response force responsibilities and requirements, funding of Antiterrorism, FP and Physical Security Programs and the applicability and capability to execute EM requirements on their non-traditional installations/separate facilities. AMC recommends use of mass notification systems and training insider threat response.
- United States Army Pacific Command raised an issue with exercises. They suggested conducting at least three exercises annually to ensure EM functionality exists and capabilities are synchronized. The Army encourages installations to conduct multiple exercises annually; however, current funding levels support one or less exercises per year.
- United States Army Europe (USAREUR) sees no gaps in ARs and finds clear guidance to implement FP and EM programs. USAREUR has clear lines of C2. It has established MAAs with Host Nations for EM support.
- The Fort Hood AIRT in coordination with HQDA elements analyzed the data from the ASCCs' and recommends the following:
  - Establish a working group no later than October 2010 to address concerns about unclear guidance in existing FP and EM Regulations. Lead: G-3/5/7. Support: OPMG and ACSIM. The working group would identify and assess existing training and education programs, research current doctrine and policy and determine if modifications are necessary. The working group will complete doctrine and policy reviews no later than December 2010. FOC during January 2014 will enable installations worldwide to employ and sustain DoD IEM Program capabilities consistent with Federal, DoD component policy, guidance and standards.
  - To address insider threat concerns, G-3/5/7, G-2 and OPMG analyze the recommendations of the Defense Science Board (DSB) study of insider threat programs when it concludes, no later than March 2011, identify and potentially adopt best practices. Lead: G-3/5/7; Support: G-2, OPMG.
  - The Deputy Chief of Staff, G-2 will develop a concept paper to support HQDA G-3/5/7 in developing an Army Threat Management Unit (ATMU), as a subordinate element of the G-34, by March 2012, to serve as a fusion center for threat information. To support the ATMU, G-2 and the U.S. Army Intelligence and Security Command (INSCOM) will develop processes and mechanisms to capture, analyze and fuse insider threat data generated via reporting requirements as defined in AR 380-67, Personnel Security Program, AR190-45, Law Enforcement Reporting and AR 381-12, Threat Awareness and Reporting Program and Army CI/LE Center standard operating procedures (SOP) to facili-

tate reporting, tracking, analysis and management of CI, law enforcement and security-related insider threats. Lead: G-2, Support: G-3/5/7 and OPMG.

- Establish a working group no later than August 2010 to address MEDCOM concerns about unclear reporting requirements and C2 issues. Lead: G-3/5/7, Support: MEDCOM and Joint Task Force National Capital Region Medical and other DRUs and ASCCs as required. The working group will analyze uncertainties in reporting requirements and issue clarifying messages not later than February 2011

- Standardize MWN systems in a "program of record" for FY 2012. Fort Hood AIRT's analysis of the Army survey of existing MWN systems from August 2009 and February 2010 revealed that Army installations had some form of Mass Warning Notification system. 211 Army installations had no central funding source or minimum standard. Lead: G-3/5/7, Support: ACSIM.

- General Order No. 9, dated September 2003, provides that G-3/5/7 is the functional proponent for FP. Army Directive (2008-02, Army Protection, see appendix E) assigns the G-3/5/7 responsibility, as the Army proponent, for Protection policy, priorities and resources for the Army. In order to meet the goals and objectives identified in Army Directive 2008-02, the G-3/5/7 recommends the Army resource a G-34 staff element to synchronize, integrate, coordinate and manage protection policies and funding. As envisaged by the G-3/5/7, a G-34 staff element will provide:

  - Unity of purpose and effort between otherwise disparate and confusing protection programs currently operating in independent lines outside of the G-3/5/7.

  - Align protection functional areas and the associated 90 disparate Management Decision Packages (MDEPs) under a single entity to provide unity of effort for safety and security.

THE G-3/5/7 RECOMMENDS the Army resource a G-34 staff element to synchronize, integrate, coordinate and manage protection policies and funding

  - Synchronize protection-related functions and create a coherent program that protects Soldiers, Families, civilians, infrastructure and information.

  - Address AMC and TRADOC concerns about response force requirements and responsibilities and Protection related funding and EM requirements.

G. Best Practices Identified by the Fort Hood AIRT.

- The G-3/5/7, Department of the Army Military Operations, Operations Directorate, Protection Division with the direct support from OPMG, performs Protection Assessments of all ACOMs, DRUs and ASCCs once every three years. These Protection Assessments review Anti-Terrorism, Intelligence, Physical Security, Law Enforcement, Military Working Dogs, Information Assurance, Information Operations, Continuity of Operations, EM and Critical Infrastructure-Risk Management. Each year the Protection Division publishes an ALARACT message regarding protection trends and best practices and identifies points of contact within each subject area.

- The Army established the CSF directorate on 1 October 2009. The CSF Program focuses

on five (5) dimensions of Soldier strength: physical, spiritual, emotional, social and family.

- Red River Army Depot Civil Support Team training. The depot sponsors 2 to 4 collective lane training events each year in support of ARNORTH and the surrounding states. The Army National Guard's Civil Support Team training meets States' requirements for certifying their assigned Civil Support Teams and fosters cooperation and camaraderie which benefits response to FP and mass casualty events.

- Holston Army Ammunition Plant entered into four (4) Memoranda of Understanding with primary city and county law enforcement, fire, rescue services and the Nuclear Security Administration. The memoranda are reviewed annually and updated when signatories change. In addition, community cooperation with other agencies (i.e., park service, school boards, hospitals, Hazardous Materials, Homeland Defense, the FBI, the United States Army Reserve and the Tennessee Army National Guard) is commendable.

- AMC's FP team adopted the Holston Army Ammunition Plant model of partnership and cooperation with local authorities in conducting annual emergency response exercises as its standard. Holston's exercise program, and now AMC's, is a model for all "Government-Owned, Contractor-Operated" installations and facilities across the Army to emulate.

- At Holston Army Ammunition Plant, Senior Leaders empower first line supervisors as "case managers" for all employee injuries or deaths. The case manager remains on the case until resolution of all issues regarding injury or death.

- Holston Army Ammunition Plant makes use of innovative partnerships with industry to acquire, at no cost, off-the-shelf or experimental capabilities in exchange for serving as the test site for industry experiments. A current partnership is providing efficient river security radar and detection equipment to help secure a portion of the Holston River that travels through Holston Army Ammunition Plant property.

- The Florida Army National Guard uses a FP compliance worksheet that is an essential component of their FP assurance process. The worksheet takes into consideration a unit's self assessment, the higher headquarters' assessment and the inspector's assessment in an effort to ensure that the most important criteria are weighted more heavily. The process also culls out the "no gos" on a separate worksheet to identify and prioritize corrective actions.

- The Nevada Army National Guard PM publishes a situation intelligence report prior to special events. The report provides situational awareness and threat analysis for criminal, extremist and international terrorist threats specific to the event. The report also includes recommended protective measures to mitigate identified threats.

- Fort Bliss Army Community Service (ACS) has nine teams each consisting of 6-7 members designated as Readiness Assessment Modules/FAC Teams representing a cross section of ACS programs. Front Desk personnel and Critical Incident Stress Management Teams are identified separately as teams. Given their presence at the entrance to the building, Front Desk personnel serve also as a first-line security team, checking patrons' identification cards and ensuring visitor sign in upon entrance. The Critical Incident Stress Management team responds solely to mass casualty, shooting incidents and other crisis situations. These teams receive monthly FAC operations training.

- Fort Leonard Wood's installation staff participates in the Missouri Information Analysis Center quarterly meetings to discuss threats and FP. The Missouri Highway Patrol di-

rects this information fusion center and includes representatives of: the Department of Homeland Security, local/federal law enforcement and intelligence organizations. The Center also "pushes out" time sensitive FP and threat information, such as "Be On the Look Out" lists.

- The robust and cooperative disaster recovery plan governing Red River and Anniston Army Depots protects information technology (IT) servers and users' data. To mitigate an event causing a total loss of critical electronic information at both depots; Red River Army Depot sends its backups to Anniston Army Depot; and Anniston in turn sends its back up to Red River Army Depot.
- Mandatory adoption of Web EOC as the system of choice in the State of Texas. The system facilitates Red River Army Depot's information and COP sharing with its surrounding communities.

Chapter 3. Major Areas of the DoD Independent Review Panel Report

AS OF JULY 2010, the Army has implemented 21 of the 79 recommendations.

A. Overview.

The Fort Hood AIRT conducted a thorough analysis of each of the recommendations in the DoD Independent Review panel report, ranking recommendations based on importance and developing an implementation plan for each of the recommendations. As of July 2010, the Army has implemented 21 of the 79 recommendations. The subsequent paragraphs provide narrative comments regarding the implementation of the DoD Independent Review Panel's recommendations. Detailed implementation plans including: recommended lead and supporting agencies, DOTMLPF solutions; in addition to rough order of magnitude resource information for the recommendations in the DoD Independent Review Panel report are in Appendix D.

B. Personnel.

The ASA(M&RA)/Army G-1 (G-1) identified 27 Independent Review Panel Report findings and recommendations within its purview. Of these, the Army implemented three recommendations: 2.3, 2.5.D and 2.12 by issuing policy guidance and curriculum changes. The Army needs DoD guidance on the remaining 24 recommendations in order to fully implement.

In its internal review, the Army found that the Service possessed sufficient policy guidance for implementing day-to-day personnel support programs and services. However in some cases, personnel policy guidance and programs require update to address unique requirements such as mass casualty, crisis incidents, workplace violence and religious accommodation. The Army continues to work with the USD(P&R) to identify indicators of violence that affect implementation of recommendations 2.1, 2.5, 2.6, 2.7, 2.8, 2.9, 2.13, 2.14, 2.15 and 2.16. We note that installation and installation commanders rated survey recommendations 2.2A (evaluate background check policies and issue appropriate updates) and 2.10 (establish a consolidated criminal investigation and law enforcement database) as having high impact.

C. Force Protection.

The G-3/5/7 and the OPMG identified within its purview twelve Independent Review Panel Report findings and recommendations. The Army needs DoD guidance on all twelve recommendations in order to fully implement. The team developed a draft implementation plan pending the DoD's guidance.

In its internal review, the Army found that the Service possessed sufficient policy guidance for implementing day-to-day FP programs. However in most cases, FP policy guidance and programs require updates to address unique requirements such as behavioral indicators, real time information sharing, integrated FP policies, internal threats, screening strategies and capabilities.

The Fort Hood Internal Review Team developed recommendations through extensive analysis, which included visits to seventeen installations worldwide. The team collected input from installation commanders during these visits to assess the potential positive impact that the implementation of the recommendations will have on installations. The Fort Hood AIRT conducted a detailed analysis of implementation requirements for each recommendation included in Appendix D.

D. Information Sharing.

The focus of the findings and recommendations in the Information Sharing area was the lack of policy, procedures and systems for the sharing of threat related information between the Services, Combatant Commands, DoD and other federal agencies such as the FBI. The inadequacy of information sharing between critical components of DoD's FP enterprise was the common thread between each of the four findings and seven recommendations in this area. The specific findings, the DoD way ahead and Army's recommended actions to implement the recommendations are below:

The DoD's commitment to support Joint Terrorism Task Forces (JTTFs) is inadequate. Action: DoD Participation with the JTTFs provides DoD with the opportunity to have access to front line information on the US counterterrorism effort. Because of this finding, DoD proposed an increase of JTTF positions so that they will eventually be represented in 85 of the 104 JTTFs across the country. DoD requested an increase from the current 60 positions resourced, with Army requesting 17 additional CI agent positions and 9 U.S. Army Criminal Investigation Command (CID) investigator positions

THERE IS NO FORMAL GUIDANCE standardizing how to share FP threat information across the Services or Combatant Commands.

added to the JTTF manning effort. Additionally, the Army requested 8 Army CI agent authorizations for placement within FBI Headquarters activities to work in the threat management unit, which will improve information sharing between the National JTTF and Army. FBI requested that DoD make this request for additional manpower within their headquarters in order to further integrate DoD into the FBI counter-terrorism (CT) effort. The Army forwarded the final manpower request to ASD (HD&ASA) for submission to SECDEF this fall in time for the FY 12 program submission.

There is no formal guidance standardizing how to share FP threat information across the Services or Combatant Commands. Action: Policy exists stating the requirement to share threat information with the Combatant Commands. However, there is no standard method for military criminal investigative organizations or CI organizations (outside a JTTF) to share threat information pertaining to a CONUS asset or individual with the geographic combatant commands. United States Northern Command (NORTHCOM) and Joint Intelligence Task Force-Counterterrorism (JITF-CT) and

the Defense Intelligence Agency (DIA) have expressed dissatisfaction with past sharing of FP and terrorism threat information from the Services. Investigative and CI organizations are reluctant to share sensitive investigative information until they receive assurances regarding the management of this data to protect the validity of open investigations. Investigative data often consists only of allegations, which are investigated to determine if valid, threat related, or connected to foreign terrorists. The Army shares immediate threat information with Commanders by the most expeditious means possible. However, investigative information may not indicate an immediate threat and require further analysis to determine potential linkages to future threat. The Army agreed with the future solution that JITF-CT and NORTHCOM will identify their FP information requirements by 31 Jul 2010. The Office of Primary Responsibility (OPR) ASD (HD&ASA), in coordination with Undersecretary of Defense (Intelligence) (USD(I)), will levy these requirements upon the appropriate DoD intelligence, CI and criminal investigative components through existing collection requirements management systems. The OPR, in coordination with USD(I) and the Assistant to the Secretary of Defense-Information Operations, will establish policy and procedures for defense intelligence col-

DOD COMMITTED TO DEVELOPING A TECHNICAL SOLUTION providing Secret Internet Protocol Router Network (SIPRNET) access to classified Guardian data residing on FBInet for intelligence community activities supporting CT/FP.

lection, CI and investigative organizations to collect, retain and disseminate FP threat information in response to combatant commander, Service and defense intelligence analytical agencies' requirements by 31 Oct 2010. JITF-CT and NORTHCOM are developing internal procedures to handle and protect investigative information. Additionally, USD(I) will endorse JITF-CT, in accordance with its charter and established authorities, as the lead for facilitating selective access to terrorism related information by designated organizations for analytic and warning requirements. Army participated fully in the development of this path forward and will continue to work with ASD (HD&ASA), USD(I) and NORTHCOM to implement this solution.

The DoD does not have direct access to a FP threat reporting system for suspicious incident activity reports. Action: DoD adopted the FBI's Suspicious Activity Reporting (SAR) eGuardian program as the DoD SAR standard. DoD made the decision to restrict account access to DoD Law Enforcement accredited/credentialed personnel only. DoD Law Enforcement personnel may pass information acquired through eGuardian regardless of physical location to Army CI or intelligence analysis personnel engaged the FP/CT mission. Law Enforcement personnel embedded within intelligence analysis activities, supporting the FP/CT mission-set, will have no restrictions placed upon them for account access. DoD committed to developing a technical solution providing Secret Internet Protocol Router Network (SIPRNET) access to classified Guardian data residing on FBInet for intelligence community activities supporting CT/FP. The intent is to merge Guardian SAR data with classified intelligence information to provide a more complete analytical picture. Army requested implementation of this technical solution by November 2010. Departmental criminal intelligence, for domestic terrorist/threat analysis, will be addressed for DoD by defense personnel detailed to the FBI. JITF-CT will complement this function at the Departmental level; however, their primary focus will remain foreign intelligence.

There are no FP processes or procedures to share real-time event information among commands, installations and components. Action: The Independent Review found that there are no FP processes or procedures to share unclassified real-time event information among commands, installations and components. In November 2009, Fort Hood, Texas went to Force Protection Condition (FPCON) Delta. There were no indications that the rest of the CONUS DoD forces were immediately notified of the event. Most installations found out about the event through the news media. Events that are

happening within one Area of Responsibility (AOR) should inform FP decisions in another. The requirement for a process/system to share event information in near real-time is key for alerting the force that an attack is underway. Future action to enable real-time FP information sharing: This recommendation is also being covered by new Secretary of Defense guidance to the Services directing support to combatant commanders under recommendation 3.1. Additionally, the Joint Staff (JS) will evaluate the current incident reporting systems used by the National Military Command Center (NMCC) and update Chairman Joint Chiefs of Staff Manual (CJCSM) 3150.03C, Joint Reporting Structure Event and Incident Reports, or other appropriate CJCSM no later than October 2010. By January 2011, the Services will ensure that all organizations are trained in reporting systems used by the NMCC. By April 2011, Combatant Commands will ensure there is an unclassified means to notify all DoD facilities within their AOR of a FPCON change.

E. Installation Emergency Response.

The Army identified, analyzed and addressed 22 emergency response issues from the DoD Independent Review Panel Report findings and recommendations. The Army is establishing working groups to further address areas of concern. Synchronization is the key factor in accomplishing the goals set forth by the Fort Hood AIRT. We recommend the Army establish a G-34 staff element to coordinate all protection related issues for the security of the Army. The G-3/5/7, acting as the focal point for installation protection issues, could then present a risk assessment to the senior Army leaders to either close the gap between requirements and resources or knowingly accept risk.

The Fort Hood AIRT recommends the following actions in order to implement these recommendations: establish a proponent to determine requirements, establish a program manager to oversee

DEVELOPING PROGRAMS OF RECORD for capabilities required by the DoD IEM Program FOC targets is a multi-year effort

life cycle development and budget resources to enable execution.

The DoD formalized the DoD IEM Program with the release of DoDI 6055.17 on 13 January 2009. The Army established the Army EM Program as a formal program of record on 13 March 2009 with the release of AR 525-27, *Army Emergency Management Program*. DoDI 6055.17 directs Services to achieve IOC no later than 13 January 2011 and FOC no later than 13 January 2014. IOC requirements focus on initial actions to field and utilize Installation Emergency Managers at all DoD Installations, responsible for developing and executing the IEM Program across all five phases of the emergency lifecycle: Preparedness, Mitigation, Prevention, Response and Recovery.

Developing programs of record for capabilities required by the DoD IEM Program FOC targets is a multi-year effort requiring the organization, manning, training, equipping and exercising of multiple capabilities across the EM lifecycle addressing all hazards. The G-3/5/7 develops policy, objectives and synchronizes protection input to the budget process, including EM requirements. The Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)) establishes the acquisition strategy for approved EM material systems with formal oversight and review, including cost effective system sustainment for the life-cycle-management. ACSIM establishes a baseline of installation's current on-hand capabilities, quantities and operational readiness rates. Based on current manpower authorizations and budget constraints, accelerating the implementation of the Army EM program is not possible without additional funding.

Public Laws 106-81 (Wireless Communications and Public Safety Act of 1999), 108-494 (ENHANCE 911 Act of 2004) and 110-283 (NET 911 Improvement Act of 2008) establish requirements for fielding and using E911 call taking and dispatch capabilities within the United States. E911 provides the capability for dispatch center operators to automatically receive and utilize the telephone number and address of the caller to decrease overall emergency response times for data collection at the dispatch center and information transfer to first responders.

E911 requires a well-managed telecommunications infrastructure database capable of providing Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information. A Geographical Information System (GIS) enabled Computer Aided Dispatch (CAD) terminal receives this information. E911 provides ANI/ALI information, speeding the call-taking process and automatically identifying the closest available first responder units based upon station locations and Global Positioning System (GPS) location updates from these units resulting in decreased response times and more efficient use of response assets.

Dispatch procedures are ineffective due to legacy telecommunications infrastructure on Army installations including the use of multiple conventional seven digit emergency numbers (varying by installation), the presence of multiple agency dispatch centers on a single installation, lack of supporting technology at existing dispatch centers and the dependence upon untrained and/or uncertified borrowed military and civilian manpower for staffing.

The Army is establishing an E911 working group consisting of G-3/5/7 Protection Division, ACSIM/IMCOM (Fire & Emergency Services, Law Enforcement, Physical Security and Public Works representatives), AMC, OPMG, OTSG, CIO/G-6 and TRADOC no later than July 2011. The working group will determine Army standards and requirements for E911 capabilities to include acquisition, fielding and sustaining strategies.

The Army conducted extensive research and incorporated federal, state and local law enforcement best practices into the training curriculum, including ASR, for Department of the Army Civilian Police (DACP), Security Guards and MPs. After the 9/11 attacks, the Army developed the US Army Civilian Police Academy with the mission of conducting state-of-the-art law enforcement and security skills training using proven best practices developed by civilian and military law enforcement agencies. This enables Army and DoD agencies to better perform their law enforcement, physical security, antiterrorism and FP missions. The USAMPS developed an ASR TSP in March 2010. ASR is taught during the 9-week academy and is included in the Field Training Program for Army Civilian Police and MPs. The TSP is a 14-hour training package. It was developed by SMEs at USAMPS using best practices developed by diverse law enforcement agencies such as the U.S. Secret Service, FBI and El Paso County Sheriff's Office.

The Army will train approximately 5,000 civilian police and security guards at an estimated cost of $2.1M (overtime pay). The ASR TSP was designed to provide commanders, PMs and Directors of Emergency Services a model for training their military and civilian police to respond to the threat of an active shooter or other incident involving workplace violence. A rapid revision to AR 190-56, The Army Civilian Police and Security Guard Program, will be staffed during 3rd QTR FY2010, with publishing anticipated by 31 December 2010, subject to staffing, to include this mandatory annual training requirement. AR 190-14, Carrying of Firearms and Use of Force for Law Enforcement and Security Duties, will also be revised this fall with publishing anticipated by 31 December 2010, subject to staffing, to address ASR and other acts of workplace violence for all Army military and civilian law enforcement and security personnel. Despite the absence of DoD guidance, the Services include the active shooter protocols in their civilian police and military police training.

DoD policy does not currently take advantage of successful models for ASR for civilian and military

law enforcement on DoD installations and facilities. DoD has no policy for active shooter scenarios, or an established process to quickly adopt civilian law enforcement best practices. The Fort Hood shooting case study will describe law enforcement response and interaction with installation agencies during and after an active shooter event. The impact of the Fort Hood shooting displayed the need for DoD to establish preventive measures as well as identify enhanced methods for emergency response personnel.

THERE IS NO SINGLE RESOURCE SPONSOR for MWN systems.

MWN system capabilities are a core component of the DoD IEM Program enabling commands to quickly and effectively warn the installation of emergencies and direct protective actions before, during and after an incident. Current capabilities are a mix of different systems and providers with no standard system configuration, or system control process. There is no single resource sponsor for MWN systems. Installations fielded existing systems through end-of-the-year money or other funding streams. The Army is establishing a MWN working group consisting of G-3/5/7 Protection Division, ACSIM/IMCOM (Fire & Emergency Services, Law Enforcement, Physical Security and Public Works representatives), AMC, OPMG, OTSG, CIO/G-6 and TRADOC to baseline current systems and develop an acquisition, fielding and sustainment plan to close identified gaps.

The COP capability enables commands to quickly and effectively exchange information, resource requests and coordinates response and recovery operations with civil and military partners. Common standards within the COP system allow user to interface with civil and military partners. Current capabilities include a mix of different civilian and military proprietary software systems and a selection of manual and software mapping applications. Existing MDEPs have not validated critical requirements and associated critical funding for fielding or sustainment of a COP system. The Army is establishing a COP working group consisting of G-3/5/7 Protection Division, ACSIM/IMCOM (Fire & Emergency Services, Law Enforcement, Physical Security and Public Works representatives), AMC, OPMG, OTSG, CIO/G-6 and TRADOC to baseline current systems and develop an acquisition, fielding and sustainment plan to close identified gaps.

F. Health Affairs.

The Independent Review Panel tasked the Army to review several of its medical programs and policies in the aftermath of the Fort Hood incident. In its internal review, the Army found that the Service possessed sufficient policy guidance for implementing medical care to include policies that appropriately addressed behavioral health conditions. The Army's OTSG and MEDCOM developed the Comprehensive Behavior Health System of Care Campaign Plan for incorporation into the Army Campaign Plan. Its purpose is to clearly delineate existing policies, procedures and guidance to establish minimum standards for TEM, Soldier and Health Care Provider support. The Army's OTSG and MEDCOM have implemented policy and training that address recommendations 5.1.A-C, 5.2.A-D, 5.3.A-C and 5.4.A.

Chapter 4. Quick Wins and Emerging Ideas

A. Overview.

In the course of developing implementation plans for the 79 recommendations in the DoD independent review panel report and the Fort Hood AIRT's review and assessment of installation policies

and procedures the team accomplished several "quick wins," identified several emerging ideas beyond those in the DoD Independent Review Panel's report. The emerging ideas require further action and/or assessment by the Army. The Fort Hood AIRT recommends the SICE board be the focal point for following up on actions contained in this chapter. The SICE should fully develop emerging ideas and ensure placement in the Army Campaign Plan as decision points.

The most significant issue identified by the Fort Hood AIRT is how we provide installation and senior commanders the tools they need to secure the force. Our current procedures fall short at synchronizing policy, establishing priorities and allocating resources to achieve the desired end state. The Army senior leadership is not given the opportunity to affect the security posture because our current process does not afford the opportunity for a complete portfolio review of protection related functions on a recurring basis.

The 20th Secretary of the Army, the Honorable Pete Geren, clearly designated the G-3/5/7 as the staff agent responsible for Army Protection Policy in Army Directive 2008-02 dated 09 April 2008 (see appendix E). This directive specified that "The Army G-3/5/7 is the proponent for Protection policy, priorities and resources." This directive also required that "once the Army Staff has established its synchronized Protection processes and procedures, an Army Regulation on Protection will be developed and released to clearly identify roles, responsibilities and relationships across the HQDA staff." To date, the Army has not achieved all the goals and objectives specified in the annex to Army Directive 2008-02.

The G-3/5/7 developed a detailed plan to establish a G-34 staff element (appendix F) enabling the Army to meet the goals and objectives specified in Army Directive 2008-02. Without this capability, there will be no staff element dedicated to integrate and synchronize over 90 MDEPs, 6 Program Evaluation Groups (PEGs) and numerous ARs that govern Protection functions. Given the urgency of the requirement and the time that has transpired since Secretary Geren signed this directive, we recommend the G-3/5/7 consider identifying an expert to bridge the gap as they develop the concept plan for the G-34. This expert would lead the effort for the G-3/5/7 in establishing a governance board or council to accomplish the specified goals and objectives in Army Directive 2008-02. We further recommend the G-3/5/7 provide milestones and report progress to the Senior Army Leadership on establishment of the G-34.

Additionally, the Army must adapt to procedures put in place since Secretary Geren signed Army Directive 2008-02. ACSIM has proposed changes to the 2011 Army Campaign Plan that identifies "Provide a Safe & Secure Working & Living Environment" as Major Objective 2-7 which is nested in Campaign Objective "Provide an Effective Protection Capability at Army Installations" (see appendix G). The Army should designate the G-3/5/7 as lead for Major Objective 2-7 and report progress as part of the Army Campaign Plan process. The Secretary of the Army should assign oversight to the VCSA who can leverage either the regularly scheduled Army Campaign Plan or Army Synchronization Meetings to track progress. Additionally, we recommend an annual review of the Protection function utilizing the portfolio review process.

Regardless of the path forward, we need to remain focused at providing installation commanders the tools necessary to protect the force. We need to focus this effort at the installation level and afford installation commanders the opportunity to influence the outcome. We need to develop procedures that provide flexibility to installation commanders to establish local priorities and afford the senior commander the opportunity to validate or change based on the threat assessment for their area of responsibility. The IMCOM staff could then consolidate requirements and work collaboratively with the G-3/5/7 for presentation to the ASA(I&E).

B. Quick Wins.

The team determined that each action below, if implemented quickly, would have an immediate and positive impact on Army FP and identification and mitigation of internal threats. These "quick wins" are as follows:

- The Army developed and implemented the iSalute CI reporting system via "Army Knowledge Online" and "Army Knowledge Online – Secure" internet based reporting links in April 2010. G-2 Information Sharing and CIO/G-6 developed and implemented the reporting platforms enabling any Soldier or Civilians with an Army Knowledge Online or Army Knowledge Online – Secure account to report a suspicious activity to Army CI.

- The Army transmitted instructions on 15 April 2010 for Army-wide implementation of the iWATCH Program by 1 August 2010. The Army iWATCH program, modeled after the nationwide program sponsored by the Los Angeles Police Department, is a modern version of the Neighborhood Watch program designed to promote anti-terrorism awareness across all commands, leverage every member of the Army community as a sensor and reporter of potential terrorist acts and establish SAR procedures at the local level

- The Army revised and re-titled AR 381-12 from "*Subversion and Espionage Directed Against the U.S. Army (SAEDA)*" to "Threat Awareness and Reporting." G-2(CI), Human Intelligence, Security and Disclosure Directorate updated this regulation to include additional observable indicators for espionage, terrorism and extremism. The revised regulation includes more robust reporting requirements.

- The Army expanded and refined active shooter training for the Army law enforcement community since the tragedy at Fort Hood. OPMG developed and implemented its plan to train MP personnel to the same level as DACPs through an annual law enforcement certification program reported through the Unit Status Report. Previously, active shooter training was limited to DACP who were trained to respond to active shooters both at their academy and in the field. The program was implemented on 1 April 2010 and is supported by USAMPS' release of an active shooter TSP on 19 March 2010.

- The Army's OPMG and G-3/5/7 authorized the use of jacketed hollow point ammunition for Army law enforcement and published an ALARACT message on 7 May 2010 in order to execute this initiative. This Army action provides an immediate solution to risks posed by internal threat response and active shooter scenarios. The Army's fielding of jacketed hollow point ammunition concludes a long-standing assessment of its effectiveness. The Army law enforcement community, within the CONUS and its territories only, now shares the long standing use of jacketed hollow point ammunition with the civilian law enforcement community.

- The G-3/5/7 now briefs the Army's EM Program to the attendees of the General Officer/Senior Commander Course at the Army Management Staff College, Fort Belvoir. Briefed topics include: NIMS Implementation Plan, EM Awareness, Ready Army and Risk Assessment for an All-Hazards approach. This is the first time General Officers/Senior Commanders are introduced to the details of the Army EM Plan and these briefings will ensure that senior commanders have the knowledge they need prior to an actual emergency. The Army needs to improve General Officer attendance to this course. Currently, only 56% of General Officers moving into senior commander billets have attended this course.

- The Army implemented the TEM Course at the AMEDD Center and School. This course trains behavioral health providers, related healthcare professionals and Unit Ministry Teams on TEM. This course standardizes how the Army will provide trauma management. A Field Manual (FM) addressing TEM is in draft pending publication. Two classes have been held as of this report.
- The General Officer Management Office revised General Officer assignment orders to expressly reflect senior commander authorities, responsibilities and duties.
- Army OTSG and MEDCOM implemented Care Provider Support training. Care Provider Support training is an annual requirement for all healthcare providers and teaches healthcare providers how to manage the unique stressors associated with providing health care. MEDCOM monitors completion through the Digital Training Management System.
- The United States Army Crime Center in concert with the FBI CJIS amended the CJIS Security Policy, June 2007, Version 4.4 (4.5 is pending review and approval for release) authorizing Private Contractor (i.e. CSGs) User Agreements to allow NCIC access for Private Contractors. Private Contractors shall be permitted access to CJIS record information systems pursuant to an agreement which specifically identifies the contractor's purpose and scope of providing services for the administration of criminal justice. Radford Army Ammunition Plant and Military Ocean Terminal Concord were the first to request access.

THE DEPUTY CHIEF OF STAFF G-3/5/7 should publish incident reporting procedures and policy from installation level to HQDA

C. Emerging Ideas.

The Fort Hood AIRT recommends inclusion of the following actions and issues in the Army Campaign Plan as decision points:

- The Deputy Chief of Staff G-3/5/7:
  - Publish incident reporting procedures and policy from installation level to HQDA. The policy must include Regular Army, Army National Guard and Army Reserve reporting requirements. The policy must also consider dual reporting from active installations to both NORTHCOM and IMCOM. Codify Army National Guard reporting as being to National Guard Bureau (NGB) with NGB disseminating to other Commands and HQDA.
  - Review Army policy to ensure EM exercise guidance includes language directing installations to integrate exercises with federal, state, local and private EM organizations into exercises to the greatest extent possible.
- The Provost Marshal General:
  - Issue policy that clearly delineates the authorities and responsibilities of CSGs in response to an active shooter scenario.
  - Establish a standard equipping package for all DA security personnel (i.e., DACP, DASGs and CSGs).
- The Deputy Chief of Staff, G-8, ensure funds are programmed for sustainment of EM

personnel and equipment. The team noted that while equipment has been procured for installation EM, in particular MWN devices, resources have not been programmed to sustain these systems over time. The lack of programmed funding for sustainment/repair of EM equipment causes equipment to remain not mission capable for a lengthy period of time until funds are reprogrammed/reallocated to pay for the cost of repair. The team recommends that the ACSIM ensure all installation EM equipment have sustainment funding programmed at the time of procurement and that procurement of new EM equipment be prohibited without the requisite sustainment funding.

- OPMG conduct a cost-benefit analysis (CBA) to determine the best means for FP and security (DACP, DASGs and CSGs) on Army installations. Ensure the CBA considers the inability of CSGs to obtain law enforcement threat information (i.e., eGuardian, NCIC, etc.).

- The Secretary of the Army direct the establishment of an Army funding line for centralized management of EM equipment and the Army Acquisition Executive appoint a Program Manager(s) with resources and authority for life cycle management of EM equipment. The Army must designate this equipment as "programs of record" and program the funding necessary to achieve both IOC and FOC as outlined in current (Department of Defense Instruction) DoDI and the NIMS and NRF. Currently, installation commanders identify and prioritize EM equipment they need. Equipment is not direct funded, procured locally and must compete for sustainment. The decentralized process results in inadequately funded and sustained EM equipment at the installation level with minimal visibility of EM equipment issues at the headquarters level.

- IMCOM establish a Battle Command Training Program for installation commanders and staffs similar to the one for Brigade Combat Teams, Divisions, Corps and ASCCs. The training would be conducted to create experiences enabling the Army's senior commanders to develop current and relevant installation command protection instincts and skills.

- The General Officer Management Office report to the VCSA attendance statistics for attendees of the General Officer/Senior Commander Course in order to improve the current attendance figures from the current 56% to 100% of senior commanders.

Appendix A (Secretary of Defense Memo, 29 January 2010, Subject: Follow-on Actions on the Findings and Recommendations of the DoD independent Review Related to the Fort Hood incident) to Fort Hood Army Internal Review Team Report

SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JAN 29 2010

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Follow-on Action on the Findings and Recommendations of the DoD Independent Review Related to the Ft. Hood Incident

The tragic shooting of U.S. military personnel at Ft. Hood, Texas on November 5, 2009 exposed deficiencies in the Department's ability to identify internal threats, its force protection programs, its emergency response procedures, and its ability to provide care to victims and families after a mass casualty situation. I established the DoD Independent Review Related to Ft. Hood to begin to identify and address relevant gaps and deficiencies in these areas. On January 13, 2010 the Review Panel co-chairs submitted their report and provided a list of findings and recommendations.

To address the breadth and complexity of the issues identified by the Independent Review Panel, I am directing a follow-on review to determine appropriate implementation of corrective actions recommended by the Review Panel. Accordingly, I designate the Assistant Secretary of Defense for Homeland Defense, Dr. Paul Stockton, to lead the follow-on review effort on my behalf.

The purpose of the follow-on review will be to thoroughly but expeditiously consider each of the findings and recommendations made by the Independent Review Panel and in turn, recommend specific implementation action as appropriate. An interim report will be due to me within 45 days and final report within 120 days.

The Independent Review also made recommendations regarding accountability matters. I have forwarded those recommendations to the Secretary of the Army for his review and action as he deems appropriate. The follow-on review directed by this memorandum will not address matters of accountability.

In addition, I direct the Secretaries of the Military Departments, Combatant Commanders and the heads of the other Department of Defense components, informed by the report of the Independent Review Panel, to initiate internal reviews in support of the follow-on review. These reviews are to assess their organization's ability below the headquarters level to identify internal threats and force protection and emergency response programs, policies and procedures. Please provide Assistant Secretary Stockton the final results upon completion.

OSD 01219-10

Appendix A

Ensuring the Department can protect its employees from the full range of threats is of critical importance. Hence, it is essential that the Department act thoughtfully but expeditiously on recommendations made by the Independent Review Panel. I expect all DoD Components to fully support the efforts of the follow-on review in carrying out this task.

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

Appendix B (Fort Hood AIRT Charter) to Fort Hood Army Internal Review Team Report

Department of Defense
Fort Hood Army Internal Review Team
Charter

April 19, 2010

1. **Purpose:** The Fort Hood Army Internal Review Team (Fort Hood AIRT) is an intra-Army departmental committee designed to 1) assess the Army's ability to identify internal threats, force protection and emergency response programs, policies and procedures and prepare a draft report of the team's findings for submission to the Assistant Secretary of Defense (Homeland Defense and America's Security Affairs); 2) review and develop an implementation plan for those findings and recommendations published by the Department of Defense (DoD) Independent Review Panel in their January 2010 report titled, "Protecting the Force: Lessons Learned from Fort Hood," that are approved by the Secretary of Defense, and; 3) recommend additional actions to be implemented by the Army and/or other Services that were not recommended by the DoD Independent Review Panel. The scope and importance of this review cause the team's objectives to exceed the capabilities of normal staff processes.

2. **Background:** On 5 November 2009, an Army Major is alleged to have opened fire at the Soldier Readiness Center at Fort Hood, Texas. Thirteen people were killed and 43 others were wounded or injured. While the response to the incident was prompt and effective, the tragedy naturally raised questions about DoD's preparedness to prevent or defend against internal threats. Immediately following the shooting, Defense Secretary Robert M. Gates established the DoD Independent Review Panel. In January 2010, the DoD Independent Review Panel published its report setting forth approximately eighty findings and recommendations, divided into five major areas: personnel, information sharing, force protection, installation emergency response and health affairs. On 29 January 2010, in a memorandum entitled, "Follow-on Action on the Findings and Recommendations of the DoD Independent Review Related to the Ft. Hood Incident," the Secretary of Defense directed each Military Department to initiate internal reviews based on the report of the DoD Independent Review Panel. The Fort Hood AIRT is established to comply with this directive. The Secretary of the Army verbally directed me to establish a committee to conduct the Army's internal review. On 1 March 2010, I appointed MG Robert Radin to lead the Fort Hood AIRT. The Fort Hood AIRT's team members were appointed on 2 March 2010 and their initial meeting was held on 3 March 2010.

3. **Mission:**

   a. Assess the Army's ability below the headquarters level to identify internal threats, force protection and emergency response programs, policies and procedures and prepare a draft report of the team's findings for submission to the Assistant Secretary of Defense (Homeland Defense and America's Security Affairs).

Appendix B

b. Develop an action plan, for Senior Army Leader approval, to implement those findings and recommendations of the DoD Independent Review Panel Related to Fort Hood ultimately approved by the Secretary of Defense.

c. Develop recommendations and corresponding implementation plans for any actions not recommended by the DoD Independent Review Panel that the Fort Hood AIRT determines will facilitate the Army's ability to improve identification of internal threats, force protection, or emergency response capabilities.

4. **Objectives:**

a. Coordinate and obtain data from Army installations to assess the Army's ability below the headquarters level to identify internal threats, force protection and emergency response programs, policies and procedures.

b. Prepare a draft report for submission to the Assistant Secretary of Defense (Homeland Defense and America's Security Affairs) assessing the Army's programs, policies, and procedures for the identification of internal threats, force protection, and emergency response.

c. Act as the Army lead for coordination with the Office of the Secretary of Defense staff involving the Services' follow-on review of the DoD Independent Review Panel's findings and recommendations.

d. Conduct a comprehensive review of the DoD Independent Review Panel findings and recommendations and develop an implementation plan for those recommendations approved by the Secretary of Defense.

e. Critically evaluate whether there are any other actions that will facilitate the Army's ability to improve identification of internal threats, force protection, or emergency response capabilities, and develop recommendations and an implementation action plan for Senior Army Leadership approval.

f. Work collaboratively with other Services' subject matter experts (SMEs) and Federal agencies to determine and implement the best practices and solutions in each of the five topic areas: personnel, information sharing, force protection, installation emergency response and health affairs.

g. Identify immediate and enduring Army policy and doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) solutions that will enable the Army's efforts to prevent similar incidents from occurring.

h. Identify immediate and enduring HQDA policy and DOTMLPF solutions that will assist the Army to more effectively react to a similar future incident should it occurs.

2

Appendix B

5. **Date to be Terminated.** The Fort Hood AIRT will terminate once it submits the *Fort Hood Internal Review Team Report* to me.

6. **Members:** The primary members of the AIRT are senior representatives (O-6 or civilian equivalent) from key HQDA staff elements and proponent stakeholders in each of the five topic areas: personnel, information sharing, force protection, installation emergency response and health affairs. All members are full-time officers and members of the Army. Primary members are assigned full-time to the Fort Hood AIRT, located at 1E124, with duties as specified by the Team Lead. Primary members must have unencumbered access to their respective staff/agency principals for immediate decision authority to execute Fort Hood AIRT actions. Supporting members will work from their home offices but will provide immediate dedicated support to the Fort Hood AIRT, as requested. The Fort Hood AIRT will operate as an independent committee without any committee organizations operating above or below it.

Primary Members:

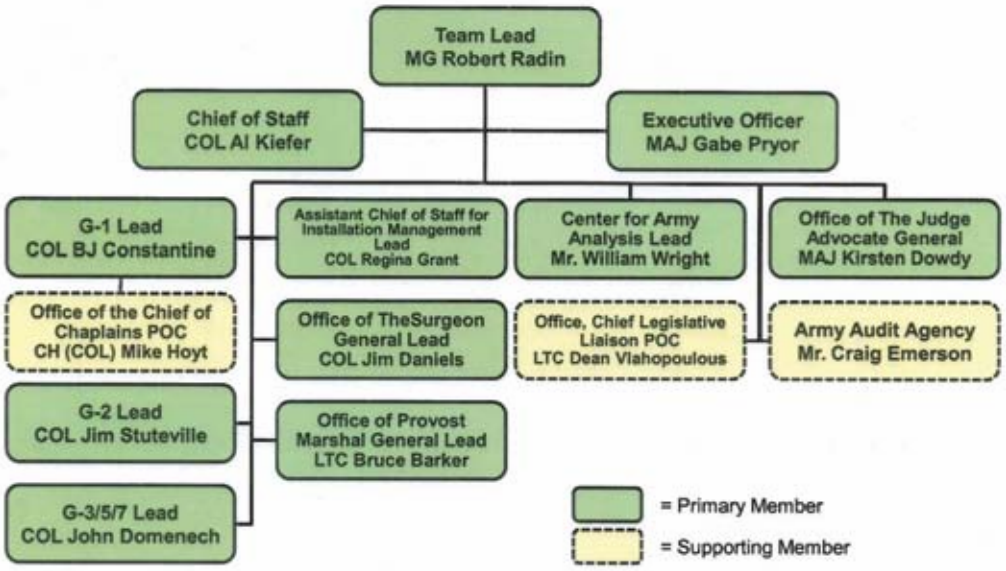
a. Team Lead
b. Executive Officer
c. Chief of Staff
d. ASA(M&RA) (1)
e. G-3/5/7 (1)
f. G2 (1)
g. OTSG (1)
h. ACSIM (1)
i. G8 CAA (1)
j. OTJAG (1)
k. OMPG (1)

Supporting Members:

a. OCCH (1)
b. OCLL (1)
c. USAAA (1)

3

Appendix B



7. **Administrative Support:** The Director of Army Staff (DAS) will formally task the Army Staff to provide the personnel and administrative support needed by the AIRT. The Office of the DAS is responsible for funding all team-related activities. The Fort Hood AIRT is a top priority.

8. **Coordinating Instructions:** The Fort Hood AIRT shall coordinate all Army Staff/ agency correspondence, reporting, and programmatic changes through the DAS prior to sending them to me. The DAS and I will provide direction to the Fort Hood AIRT.

9. **Frequency of Meetings:** The Fort Hood AIRT will meet as directed by the Team Lead.

10. **Product:** NLT 15 June 2010, the Fort Hood AIRT shall provide me with a *Fort Hood Internal Review Team Report* which includes a draft report of the team's findings for submission to the Assistant Secretary of Defense (Homeland Defense and America's Security Affairs) detailing the Fort Hood AIRT's assessment of the Army's ability to

4

Appendix B

identify internal threats, force protection and emergency response programs, policies and procedures. This report shall also provide an implementation plan for those DoD Independent Review Panel recommendations that are approved by the Secretary of Defense. Finally, this report should provide recommendations and corresponding implementation plans for any actions not recommended by the DoD Independent Review Panel that the Fort Hood AIRT determines will facilitate the Army's ability to improve identification of internal threats, force protection, or emergency response capabilities.

FOR THE SECRETARY OF THE ARMY:

PETER W. CHIARELLI
General, U.S. Army
Vice Chief of Staff

5

Appendix C (Army Vice Chief of Staff Tasking Memo) to Fort Hood Army Internal Review Team Report

FOR OFFICIAL USE ONLY

DEPARTMENT OF THE ARMY
OFFICE OF THE VICE CHIEF OF STAFF
201 ARMY PENTAGON
WASHINGTON DC 20310-0201

APR 19 2010

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

1. Situation.

a. General. On 5 November 2009, a gunman opened fire at the Soldier Readiness Center at Fort Hood, Texas. Thirteen people were killed and 43 others were wounded or injured. The tragedy raised questions about the degree to which the entire Army is prepared for similar incidents in the future-especially multiple simultaneous incidents. Following the shooting, the Secretary of Defense established the Department of Defense (DoD) Independent Review Related to Fort Hood to identify and address possible deficiencies in the:

- DoD's programs, policies, processes, and procedures related to force protection and identifying DoD employees who could potentially pose credible threats to themselves and others;
- sufficiency of the DoD emergency response to mass casualty situations at DoD facilities and the response to care for victims and families in the aftermath of mass casualty events;
- sufficiency of programs, policies, processes, and procedures for the support and care of healthcare providers while caring for beneficiaries suffering from Post Traumatic Stress Disorder or other mental and emotional wounds and injuries;
- adequacy of Army programs, policies, processes, and procedures as applied to the alleged perpetrator.

On 15 January 2010, the DoD Independent Review Panel issued a report entitled "Protecting the Force: Lessons from Fort Hood." The DoD report contains 79 recommendations for the DoD to consider for implementation. On 29 January 2010, the Secretary of Defense designated the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs ASD(HD&ASA) as the lead for the DoD follow-On review effort and directed the Service Secretaries to: "initiate internal reviews in support of the follow-on review;" and "assess their organization's ability below the headquarters level to identify internal threats and force protection and emergency response programs, policies, and procedures." In order to facilitate the Army' follow-on internal review requirement, I appointed Major General Robert Radin to lead the Fort Hood Army Internal Review Team (AIRT).

b. References.

(1) Report of the DoD Independent Review, "Protecting the Force: Lessons Learned from Fort Hood," The Honorable Togo Dennis West, Jr. and Admiral Vern Clark, U.S. Navy (Ret.), 15 January 2010.

FOR OFFICIAL USE ONLY

Appendix C

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

(2) Secretary of Defense memorandum dated 29 January 2010, Subject: Follow-on Action on the Findings and Recommendations of the DoD Independent Review Related to the Fort Hood Incident.

(3) Action memorandum, 18 February 2010, Subject: Department of Defense (DoD) Ft. Hood Follow-on Review Task Force.

c. Applicability. This tasking memo applies to Headquarters, Department of the Army (HQDA) Staff, Army Commands (ACOMs), Army Service Component Commands (ASCCs), Direct Reporting Units (DRUs), and supporting agencies and activities.

2. Mission. The Army will:

a. Develop a plan to implement the Independent Review Panel's recommendations as approved by the Secretary of Defense.

b. Identify corresponding recommendations developed as a result of the Army's analysis into the Independent Review Panel's recommendations, incorporating additional recommendations approved by the Secretary of the Army into the implementation plan.

c. Conduct an internal review and assessment of installation level programs, policies, and procedures for identifying internal threats, force protection, and emergency response and prepare a draft report of the team's findings for submission to the ASD(HD&ASA).

3. Execution.

a. Intent. My intent is to meet the guidance of the Secretary of Defense, Secretary of the Army, and the Chief of Staff, Army, to evaluate the findings and recommendations of the Independent Review Panel's Report to improve programs, policies, and procedures for identification of internal threats, force protection, and emergency response. The Army will analyze the DoD report's findings and recommendations; correct deficiencies; and adjust, synchronize, integrate, and institutionalize all Policy, Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Resources (P-DOTMLPF-R) solutions across the Army.

(1) End State.

(a) All approved recommendations implemented and sustainable within existing Army forums.

(b) A recurring review and assessment program of installation level programs, policies, and procedures to identify internal threats, force protection, and emergency response.

(c) Commanders will have the tools they need to preclude or minimize the effects of a future threat event.

Appendix C

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

(2) Objectives.

(a) Implement and institutionalize approved recommendations into P–DOTMLPF-R solutions Army-wide.

(b) Improve systems and create solutions that are sustainable over the long-term.

(c) Synchronize Army efforts internally, with other Services, and OSD.

b. Concept of Operation.

(1) General. This tasking memo formalizes the Army's efforts to improve internal threat identification, force protection, and emergency response operations. This plan will synchronize, integrate and capture the efforts of the HQDA staff, ACOMs, ASCCs, and DRUs to institutionalize P–DOTMLPF-R solutions to approved recommendations identified in the Independent Review Panel's report and other recommendations identified in on-going analysis.

(2) Phasing. We must leverage existing Army initiatives ongoing or completed. The following phases run concurrently and are completed based on individual findings and recommendations.

(a) Phase I – Assessment. This phase is in progress and consists of identifying tasks and associated implementation timelines, lead/supporting agencies, resources, strategic communication requirements, and execution tracking forums across the P-DOTMLPF-R required to implement recommendations in the Independent Review Panel's report and other identified recommendations. Additionally, during this phase the Army Internal Review Team will develop criteria for conducting internal review and assessment of installation programs, policies, and procedures for identifying internal threats, force protection, and emergency response.

(b) Phase II – Initial Implementation. Phase II operations focus on implementing recommendations in the short term (6-12 months), continuing task development for recommendations requiring a long-term period (>12 months) to implement, and conducting an installation level program, policy, and procedure review and assessment.

(c) Phase III – Final Implementation. This phase begins when the Army follow-on review report is published. Phase III operations focus on monitoring the execution of tasks required to implement the recommendations in the follow-on review report.

(d) Phase IV – Institutionalization. This phase begins when the Director of the Army Staff (DAS), as reported to him by HQDA Staff, ACOMs, ASCCs, and DRUs determines that all approved recommendations have been implemented across the P-DOTMLPF-R. This phase ends when the DAS determines, in coordination with HQDA Staff, ACOMs, ASCCs, and DRUs, that all implemented recommendations are institutionalized within Army programs, policies, and procedures.

Appendix C

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

(3) Framework. The oversight, integration, and synchronization of all tasks required to implement recommendations will be accomplished using a framework that adds the function of policy to the Army functional structure of P-DOTMLPF-R. A recommendation matrix, using a web-based relational database program, will be updated to monitor status of implementation, ensure synchronization across the Army, and to integrate new findings and recommendations, as appropriate.

(4) Recommendation Matrix. (Annex A) All ongoing P–DOTMLPF-R tasks identified to implement recommendations (whether an Independent Review Panel or an additional recommendation identified in the analysis) will be populated in the Recommendation Database. The database facilitates implementation, synchronization, and monitoring.

(5) Monitoring Execution – The G-3/5/7, via the Army Campaign Plan, is responsible for monitoring overall execution of the Army Internal Review Team's final approved report.

(6) Shaping Operations. The communications strategy informs and educates three major audiences: critical policy and resource decision makers (Congress); Internal (DoD & Army); and key media agenda setters (who will shape public perception). Our communication priorities are: 1) to provide information to key Congressional oversight committees as directed by the CSA and coordinated with OSD-LA; 2) inform and educate Soldiers and Families as to what actions are in progress; and 3) as appropriate, provide factual, transparent information to the media.

c. Specified Tasks.

(1) Fort Hood Army Follow-on Internal Review Team Leader.

(a) As the Army lead for the Fort Hood Army follow-on internal review, coordinate, monitor, and synchronize all Army efforts to: 1) develop an implementation plan for approved Independent Review Panel and other identified recommendations and 2) develop an internal review and assessment program for installation level programs, policies, and procedures for identifying internal threats, force protection, and emergency response.

(b) Maintain the recommendation matrix (Annex A) via a supporting database.

(c) As required by the DAS, respond to Army leadership requests for information.

(d) Represent the Army at all OSD meetings pertaining to the Fort Hood Army follow-on review.

(2) Deputy Chief of Staff, G-6. Provide support to lead agencies as indicated in Annex A.

(3) Deputy Chief of Staff, G-1.

Appendix C

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

(a) Lead for DoD Independent Review Panel recommendations as indicated in Annex A. Responsible for conducting analysis and developing an implementation plan, IAW coordinating instructions.

(b) Identify additional corresponding recommendations during analysis. Develop an implementation plan for additional recommendations IAW coordinating instructions.

(c) Provide support to lead agencies as indicated in Annex A.

(3) Deputy Chief of Staff, G-2.

(a) Lead for DoD Independent Review Panel recommendations as indicated in Annex A. Responsible for conducting analysis and developing an implementation plan, IAW coordinating instructions.

(b) Identify additional corresponding recommendations during analysis. Develop an implementation plan for additional recommendations IAW coordinating instructions.

(c) Provide support to lead agencies as indicated in Annex A.

(4) Deputy Chief of Staff, G-3/5/7.

(a) Ensure the final implementation plan is synched with the Army Campaign Plan.

(b) Lead for DoD Independent Review Panel recommendations as indicated in Annex A. Responsible for conducting analysis and developing an implementation plan, IAW coordinating instructions.

(c) Identify additional corresponding recommendations during analysis. Develop an implementation plan for additional recommendations IAW coordinating instructions.

(d) Provide support to lead agencies as indicated in Annex A.

(5) Deputy Chief of Staff, G-8.

(a) Ensure resources required to implement approved recommendations are programmed.

(b) Provide support to lead agencies as indicated in Annex A.

(6) Assistant Chief of Staff, Installation Management.

(a) Lead for DoD Independent Review Panel recommendations as indicated in Annex A. Responsible for conducting analysis and developing an implementation plan, IAW coordinating instructions.

(b) Identify additional corresponding recommendations during analysis. Develop an implementation plan for additional recommendations IAW coordinating instructions.

Appendix C

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

(c) Provide support to lead agencies as indicated in Annex A.

(7) Office of the Chief, Legislative Liaison. Provide legislative advice to the AIRT.

(8) Office of the Chief of Chaplains.

(a) Lead for DoD Independent Review Panel recommendations as indicated in Annex A. Responsible for conducting analysis and developing an implementation plan, IAW coordinating instructions.

(b) Identify additional corresponding recommendations during analysis. Develop an implementation plan for additional recommendations IAW coordinating instructions.

(c) Provide support to lead agencies as indicated in Annex A.

(9) Office of the Surgeon General.

(a) Lead for DoD Independent Review Panel recommendations as indicated in Annex A. Responsible for conducting analysis and developing an implementation plan, IAW coordinating instructions.

(b) Identify additional corresponding recommendations during analysis. Develop an implementation plan for additional recommendations IAW coordinating instructions.

(c) Provide support to lead agencies as indicated in Annex A.

(10) Office of the Judge Advocate General.

(a) Provide legal support to the AIRT as required.

(b) Provide support to lead agencies as indicated in Annex A.

(11) Office of the Provost Marshal General.

(a) Lead for DoD Independent Review Panel recommendations as indicated in Annex A. Responsible for conducting analysis and developing an implementation plan, IAW coordinating instructions.

(b) Identify additional corresponding recommendations during analysis. Develop an implementation plan for additional recommendations IAW coordinating instructions.

(c) Provide support to lead agencies as indicated in Annex A.

(12) Office of the Chief of Public Affairs. Provide public affairs support to the AIRT.

(13) The Inspector General. Provides advice on inspections to the AIRT. Be prepared to conduct follow up/compliance inspections on installation implementation of AIRT recommendations as directed by the Secretary of the Army/Chief of Staff, Army.

Appendix C

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

(14) Director, Army National Guard.

(a) Provide support to lead agencies as indicated in Annex A.

(b) Conduct an internal review and assessment of installation level programs, policies, and procedures for: identification of internal threats, force protection, and emergency response IAW with the criteria and reporting requirements in Annex B.

(c) Report results of the review and assessment to the Fort Hood AIRT G-3/5/7 representative NLT 10 May 2010.

(15) ASCCs, ACOMs, DRUs, supporting agencies, and activities.

(a) Provide support to lead agencies as indicated in Annex A.

(b) If you are an installation owning command, conduct an internal review and assessment of installation level programs, policies, and procedures for: identification of internal threats, force protection, and emergency response IAW with the criteria and reporting requirements in Annex B.

(c) Report results of the review and assessment by installation to your ASCC.

(d) ASCCs will consolidate all assessment reports in their AOR and submit to the Fort Hood AIRT G-3/5/7 representative NLT 10 May 2010.

d. Coordinating Instructions.

(1) This tasking memo is effective for execution upon receipt.

(2) Principal HQDA staff designated as a recommendation lead in Annex A are responsible for developing an implementation plan for each recommendation for which they are responsible and provide that information to their AIRT lead below NLT COB 3 May 2010. The implementation plan for each recommendation must include:

(a) Tasks required to implement each recommendation categorized IAW the P-DOTMLPF-R model.

(b) Lead/supporting agencies for each task.

(c) Linkage to other recommendations/tasks.

(d) Identification of best practices that can be used for Army-wide adoption.

(e) Performance metrics as applicable.

(f) Projected resources required to implement each task, with a final calculation provided by 31 May 2010 if required.

Appendix C

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

(g) Program Evaluation Group (PEG) responsible to program the resources for each task.

(h) Task completion milestones and completion suspense.

(i) Indicate if a task has Congressional interest.

(j) Develop a strategic communication plan for each task if necessary.

(k) Recommend an existing Army forum for tracking implementation/execution of each task.

(3) Fort Hood AIRT points of contact:

(a) Team Chief of Staff: COL Al Kiefer, 571-256-1342, allen.kiefer@conus.army.mil.

(b) ASA(M&RA)/G-1: COL BJ Constantine, 571-256-1340, bj.constantine@us.army.mil.

(c) G-2: COL Jim Stuteville, 571-256-1338, james.stuteville@us.army.mil.

(d) G-3/5/7: COL John Domenech, 571-256-1336, john.domenech@us.army.mil.

(e) ACSIM: COL Regina Grant, 571-256-1337, regina.grant@us.army.mil.

(f) OTSG: COL Jim Daniels, 571-256-1341, danielsj-hqtmp@conus.army.mil.

(g) OPMG: LTC Bruce Barker, 703-571-3316, Bruce.L.Barker@us.army.mil.

(h) OTJAG: MAJ Kirsten Dowdy, 571-256-1344, Kirsten.Dowdy@us.army.mil.

(i) OCCH: CH(COL) Michael Hoyt, 703-611-1131, Michael.hoyt@us.army.mil.

(j) OCLL: LTC Dean Vlahopoulos, 703-697-0275, dean.vlahopolous@us.army.mil.

(4) DIRLAUTH ALCON for planning and coordination. Keep the Fort Hood AIRT informed.

FOR THE SECRETARY OF THE ARMY:

PETER W. CHIARELLI
General, U.S. Army
Vice Chief of Staff

ANNEXES

Appendix C

FOR OFFICIAL USE ONLY

SUBJECT: Fort Hood Army Follow-On Internal Review Tasking Memo

A – Recommendation Matrix
B – Installation level programs, policies, and procedures assessment criteria and reporting format

DISTRIBUTION

Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Europe
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Pacific
U.S. Army Africa
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command
Eighth U.S. Army
U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Test and Evaluation Command
U.S. Army Reserve Command
U.S. Army Installation Management Command
U.S. Army Accessions Command
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center

9
FOR OFFICIAL USE ONLY

Appendix D (Implementation Plan for Recommendations in the DoD Report) to Fort Hood Army Internal Review Team Report

A. Overview: This appendix provides implementation requirements for the recommendations contained in the DoD Independent Review Panel report. The Fort Hood AIRT considered the Doctrine (D), Organization (O), Training (T), Materiel (M), Leadership and Education (L), Personnel (P) and Facilities (F) (DOTMLPF) model in determining actions required. It is important to note that all cost estimates are subject to cost-benefit analyses and submitted to ASA(FM&C) for validation.

B. ASA(M&RA)/DCS, G-1/CCH Lead:

1. **Finding 2.1 - DoD programs, policies, processes and procedures that address identification of indicators for violence are outdated, incomplete and fail to include key indicators of potentially violent behaviors.**

   Recommendation 2.1.D - (OTSG and G-3/5/7 in support) Develop programs to educate DoD personnel about indicators that signal when individuals may commit violent acts or become radicalized.

   Discussion: The Army will issue commanders and supervisors interim guidance until the DoD releases identified behavioral indicators of violence from the DSB study scheduled for completion no later than March 2011. In addition to the DSB study, the Army will integrate concepts from the FBI Behavioral Science Unit's Military Violence Unit into its violence indicator education program. The estimated timeframe for program analysis, design, development and implementation is two years.

   Key actions necessary to implement the recommendation include:

   - (D) Write, staff, adjudicate and publish an update to AR 600-20, Army Command Policy.
   - (D) Address identification of violent behavior indicators, contributing factors, or prevention of workplace violence.
   - (T) Modify existing or adopt new training requirements addressing behavioral observations and reporting.
   - (L) Work with TRADOC to develop a program of instruction for the soldier to enable him/her to effectively observe behavioral characteristics or actions that could lead to or result in violent acts.

2. **Finding 2.3 - DoD standards for denying requests for recognition as an ecclesiastical endorser of chaplains may be inadequate.**

   Recommendation 2.3A - Review the limitations on denying requests for recognition as ecclesiastical endorsers of chaplains.

   Discussion: The Army's position is that the current DoD Instruction is adequate in both scope and authority. In order to accomplish this recommendation the Service Chiefs of Chaplains through the Armed Forces Chaplain Board will review DoD Instruction 1304.28, "*Guidance for The Appointment of Chaplains for the Military Departments*."

3) **Finding 2.5 - The policies and procedures governing assessment for pre- and post-deployment medical risks do not provide a comprehensive assessment of violence indicators.**

Recommendation 2.5.A - (OTSG and G-3/5/7 in support) Assess whether pre- and post-deployment behavioral screening should include a comprehensive violence risk assessment.

Recommendation 2.5.B - (OTSG and G-3/5/7 in support) Review the need for additional post-deployment screening to assess long-term behavioral indicators that may point to progressive indicators of violence.

Recommendation 2.5.C - (OTSG and G-3/5/7 in support) Revise pre- and post-deployment behavioral screening to include behavioral indicators that a person may commit violent acts or become radicalized.

Recommendation 2.5.D - (OTSG and OTJAG in support) Review policies governing sharing healthcare assessments with commanders and supervisors to allow information regarding individuals who may commit violent acts to become available to appropriate authorities.

Discussion: The Army implemented recommendation 2.5.D. ALARACT 160/2010, dated 28 May 2010, directs specific implementation tasks and reviews to improve communication between patients and providers, commanders and patients and commanders and providers. Health care providers are authorized to provide health information to commanders as it relates to indicators of possible violence. In order to implement recommendations 2.5.A-C, the Army will assist the USD(P&R) to determine if current pre- and post-deployment screening requires additions or revision.

Key actions necessary to implement the recommendation include:

- (D) Review and update AR 600-8-101, "*Personnel Processing*" by February 2011 (G-1 lead).
- (D) Write, staff, adjudicate and publish an interim update to AR 600-20, "*Army Command Policy*" by February 2011 (G-1 lead).

4) Finding 2.6 - The Services have programs and policies to address prevention and intervention for suicide, sexual assault and family violence, but guidance concerning workplace violence and the potential for self-radicalization is insufficient.

Recommendation 2.6.A - (OTSG and ACSIM in support) Revise current policies and procedures to address preventing violence toward others in the workplace. (Note: This recommendation requires OSD action before the Army can implement)

Recommendation 2.6.B - (OTSG, ACSIM and TRADOC in support) Integrate existing programs such as suicide, sexual assault and family violence prevention with information on violence and self-radicalization to provide a comprehensive prevention and response program.

Discussion: The Army is participating with and providing input to develop DoD policy on the prevention of workplace violence. The development process phase will complete no later than January 2011. Concurrently, the Army is developing an internal workplace violence-training program similar to the Civilian Personnel Management Services' program with projected implementation no later than March 2011.

Key action necessary to implement the recommendation includes:

- (D) Develop an Army version of the Civilian Personnel Management Services' Workplace Violence Training program by March 2011 (G-1 lead).

5) Finding 2.7 - DoD policy regarding religious accommodation lacks the clarity necessary to help command-

ers distinguish appropriate religious practices from those that might indicate a potential for violence or self-radicalization.

Recommendation 2.7A - Promptly establish standards and reporting procedures that clarify guidelines for religious accommodation. (Note: This recommendation requires OSD action before the Army can implement)

Discussion: The Army will assist the Armed Forces Chaplains' Board in the development of a "*Guide to Religious Accommodation*" to provide commanders with a framework for religious accommodation decision-making. Revision of DoD Instruction 1300.17, "*Religious Accommodation,*" creates a two-tiered approach to religious accommodation request approvals.

Key actions necessary to implement the recommendation include:

- (D) Interim update AR 600-20, "*Army Command Policy*," as required by DoD Instruction 1300.17 revision by September 2011 (G-1 lead).
- (L) Integrate guidance on DoDI 1325.06, "*Handling Dissident and Protest Activities Among Members of the Armed Forces*," into Chaplain Professional Military Education by March 2011 (OCCH lead).

6) **Finding 2.9 - DoD and Service guidance does not provide for maintaining and transferring all relevant information about contributing factors and behavioral indicators throughout Service members' careers.**

Recommendation 2.9.A - (OTJAG in support) Review what additional information (e.g., information about accession waivers, substance abuse, minor law enforcement infractions, conduct waivers) should be maintained throughout Service members' careers as they change duty locations, deploy and re-enlist.

Recommendation 2.9.B - (OTSG and OTJAG in support) Develop supporting policies and procedures for commanders and supervisors to access this information. (Note: This recommendation requires OSD action before the Army can implement)

Discussion: The Army will assist in updating DoDI 1336.08, "*Military Human Resource Records Life Cycle Management*." The update for this instruction, which governs the type of records to retain, will occur no later than June 2011. Concurrently, the procedures and system to share records will be developed to facilitate implementation.

Key action necessary to implement the recommendation includes:

- (D) Review and update AR 600-8-104, "*Military Personnel Information Management/ Records*" by September 2011 (G-1 lead).

7) **Finding 2.12 - Policies governing communicating protected health information to other persons or agencies are adequate at the DoD-level, though they currently exist only as interim guidance. The Services, however, have not updated their policies to reflect this guidance.**

Recommendation 2.12A - (OTSG in support) Ensure Services update policies to reflect current DoD-level guidance on the release of protected health information.

Discussion: The Army implemented this recommendation through update of AR 40-66, "*Medical Record Administration and Health Care Documentation*," dated January 2010, and will ensure review of this regulation upon release of the anti-stigma DoDI scheduled for release by September 2010. Additionally, the OTSG and MEDCOM Policy Memorandum

10-024, "*Case Management for Soldiers Referred to the Network for Behavioral Health Care*," dated March 29, 2010, requires that Soldiers undergo behavioral health care in the network and not at a military treatment facility. Soldiers will also be required to sign an authorization that allows a case manager to access the Soldier's pertinent health information generated by a network behavioral health care provider.

Key action necessary to implement the recommendation includes:

- (D) Review and update AR 40-66, "*Medical Record Administration and Health Care Documentation*," by March 2011 (OTSG lead).

8) **Finding 2.15 - DoD policy governing prohibited activities is unclear and does not provide commanders and supervisors the guidance and authority to identify indicators of violence or take actions to prevent violence.**

Recommendation 2.15.A - (OTJAG in support) Review prohibited activities and recommend necessary policy changes.

Discussion: The Army will integrate changes from OSD's review of DoDI 1325.06, "*Handling Dissident and Protest Activities Among Members of the Armed Forces*," into AR 600-20, "Army Command Policy," within 180 days after instruction update.

Key action necessary to implement the recommendation includes:

- (D) Update AR 600-20, "*Army Command Policy*," as necessary by September 2011 (G-1 lead).

9) **Finding 2.16 - Authorities governing civilian personnel are insufficient to support commanders and supervisors as they attempt to identify indicators of violence or take actions to prevent violence.**

Recommendation 2.16.A - (OTSG and OTJAG in support) Review civilian personnel policies to determine whether additional authorities or policies would enhance visibility on indicators of possible violence and provide greater flexibility to address behaviors of concern.

Discussion: The Army will assist OSD in its effort to develop a DoD-level policy on prevention of workplace violence. Draft policy is currently undergoing informal staffing by the working group. The Army anticipates that a two-phase training program will result. Within the first two (2) years new supervisors will undergo training and refresher training will be required every three (3) for supervisors with over two years of experience. This will occur no later than May 2011 (G-1 lead).

Key action necessary to implement the recommendation includes:

- (L) Integrate Civilian Leader training into existing training programs by May 2011 (G-1 lead).

10) **Finding 4.9 - The lack of published guidance for religious support in mass casualty incidents hampers integration of religious support to installation EM plans.**

Recommendation 4.9.A - (ACSIM in support) Consider modifying DoD and Service programs designed to promote, maintain or restore health and well-being to offer each person the services of a chaplain or religious ministry professional.

Recommendation 4.9.B - (ACSIM in support) Develop policy for religious support in response to mass casualty incidents and integrate guidance with the installation EM Program.

Discussion: The Army OCCH reviewed its programs and the above recommendations and found that chaplain training, force structure distribution, command integration and regu-

lations adequately support its response. The Army, through the Armed Forces Chaplains Board, is participating in DoD's review of policies and identification of best practices for religious support to mass casualty incidents by June 2010. The Army will integrate changes arising from this review into AR 165-1, "*Army Chaplain Corps Activities*." In April 2010, OCCH integrated a change into the HQDA Mass Casualty Response Plan that designates the Army Chief of Chaplains as branch proponent to coordinate worldwide chaplain augmentation to a mass casualty site in response to command priorities.

Key action necessary to implement the recommendation includes:

- (D) Based on DoD policy review results, the Army will review and update AR 165-1, "*Army Chaplain Corps Activities,*" and update as appropriate.

11) **Finding 4.10 - Inconsistencies among Services entry-level chaplain training program can result in inadequate preparation of new chaplains to provide religious support during mass casualty incidents.**

Recommendation 4.10.A - Review mass casualty incident response training in the Chaplain Officer Basic Courses by September 2010 (OCCH lead).

Discussion: The Army implemented this recommendation. The United States Army Chaplain Center and School (USACHCS) adjusted the basic officer course curriculum to include discussion on the process and planning involved in the Fort Hood incident. The enhanced instruction began June 2010. Additionally, USACHCS implemented an hour of additional instruction into its Senior Leader course curriculum to include religious support to the installation mass casualty response SOPs, exercise planning and installation staff integration.

12) **Finding 4.11 - The DoD has not yet published guidance regarding installation or unit memorial service entitlements based on the new Congressional authorization to ensure uniform application throughout the Department.**

Recommendation 4.11.A - Develop standardized policy guidance on memorial service entitlements.

Discussion: The Army implemented this recommendation with the release of ALARACT 146/2010 on 10 May 2010. The ALARACT release provided guidance for implementation until release of the formal directive. The Army anticipates that the formal Army directive will be released by 15 November 2010.

13) **Finding 4.12 - DoD casualty affairs policy, Federal law and DoD mortuary affairs guidance do not exist regarding injury or death of a private citizen with no DoD affiliation on a military installation within CONUS. There is no prescribed process to identify lead agencies for casualty notification and assistance or to provide care for the deceased, resulting in each case being handled in an ad-hoc manner.**

Recommendation 4.12.A - Review current policies regarding casualty reporting and assistance to the survivors of a private citizen with no DoD affiliation, who is injured or dies on a military installation within CONUS. **(Note: This recommendation requires OSD action before the Army can implement)**

Recommendation 4.12.B - Review current mortuary affairs policies relating to mortuary services for private citizens who become fatalities on a military installation within CONUS. **(Note: This recommendation requires OSD action before the Army can implement)**

Discussion: The Army participates through the Casualty Advisor and Central Joint Mortuary Affairs Boards to draft appropriate policy. These boards are both scheduled to meet in October 2010.

C. Army G-2 Lead:

1) Finding 2.2 - Background checks on personnel entering the DoD workforce or gaining access to installations may be incomplete, too limited in scope, or not conducted at all.

Recommendation 2.2A - Evaluate background check policies and issue appropriate updates.

Recommendation 2.2B - Review the appropriateness of the depth and scope of the National Agency Check with Local Agency and Credit Check as a minimum background investigation for DoD Secret clearance.

Recommendation 2.2C - (G-3/5/7 Lead; see paragraph c. for details) Educate commanders, supervisors and legal advisors on how to detect and act on potentially adverse behaviors that could pose internal threats.

Recommendation 2.2D - Review current expedited processes for citizenship and clearances to ensure risk is sufficiently mitigated.

Discussion: The National Joint Security and Suitability Reform Team (NJSSRT) is revising the national investigative standards. The NJSSRT goal is to issue the revised national investigative standards by December 2010.[1] The Army concurs with the revised National investigative standards and has successfully demonstrated and implemented many of them.

While the Army remains a strategic partner and supports key initiatives of the National NJSSRT, on 23 March 2010, the G-2 submitted a formal waiver request to the USD(I) from certain existing DoD policy. Once approved, the waiver will provide the Army with additional authority to implement security measures and increase the scope of investigation for specific categories of individuals with significant foreign loyalties and connections.

The Army is working to implement Homeland Security Presidential Directive – 12 (HSPD-12)2. The implementation of HSPD-12 will mandate populations (i.e., contractors working unclassified contracts and certain non-appropriated Fund personnel), who were not previously subjected to a background investigation are properly vetted, which includes the submission of a background investigation. The G-2 will issue an ALARACT message by August 2010 that will provide clarifying guidance to Army commanders and leaders, on the reporting of derogatory information. The ALARACT message will ensure commanders understand how to report derogatory information, where to report it and the requirements associated with reporting. To alleviate risks associated with certain categories of non-US citizens entering the Army and subsequently receiving United States citizenship under the provisions of EO 13269, the Army will implement policy that will enhance the military accessions screening process for certain categories of foreign nationals with significant foreign loyalties and connections (i.e., Soldiers enlisting into Military Occupational Specialty (MOS) 09L Interpreter/Translator and Military Accessions Vital to National Interest (MAVNI)).

Key actions necessary to implement the recommendation include:

- (D) Adjustments to doctrine may be required once policy and procedures are completed. Adjustments to policy will be required.
- (O) Preliminary working groups have identified specific organizations that are best suited to promulgate policies and procedures. The Army will consider adjustments to these organizational structures once policy and procedures are identified within the DoD and Army working groups.

[1]On February 16, 2010 the Joint Security and Suitability Reform Team issued a comprehensive Strategic Framework to Congress, that framework includes a strategic communications plan that articulates the goals of security clearance reforms across the federal government.

[2]HSPD-12 issued in 2004, mandates all persons issued a Personally Identifiable Verification Card (Common Access Card) for long term access (>6mos) to a Federal installation or access to a Government IT system be subjected to a National Agency Check with written inquiries (NACI). A NACI comprises of FBI checks, as well as written inquires to local law enforcement officials that covers the past 5-7 years where an individual was employed or resided.

- (T) Ensure that leaders train Soldiers to identify and report Soldiers that exhibit indicators of potential violence and/or potential terrorist behavior consistent with the 23 November 2009 ALARACT message 322/1009 which directed that all commanders review measures to prevent and mitigate potential acts of violence directed against the Army.
- (M) The Army will fully implement the Army Investigative Enterprise Solution (AIES) for the efficient and effective processing of background investigations to the Office of Personnel Management (OPM). Army implemented eScreening capability, which reviews all background investigations completed by OPM and submitted to the Army Central Clearance Facility (CCF). The eScreening review automatically identifies and highlights issues of security and CI concern for subsequent action.
- (L) The Army will issue an ALARACT message to provide clarifying guidance to Army commanders and leaders on how and where to report derogatory information by August 2010.
- (P) Army Accessions Command will participate in a pilot program to demonstrate the automatic records check capability.

Resource Estimate ($ in Millions)

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
Security Technicians	266	Research						
Adjudicators	183	Analysis						
IT/Staff Officers	12	Support						
Total	461		95	76.2	76.2	76.2	76.2	76.2

2) Finding 2.4 - The DoD has limited ability to investigate Foreign National DoD military and civilian personnel who require access to DoD information and systems and facilities in the US and abroad.

Recommendation 2.4 - Coordinate with Department of State and OPM to establish and implement more rigorous standards and procedures for investigating Foreign National DoD Personnel.

Discussion: If we are to strengthen the background investigation program, the Army recommends that the USD(I) and the USD(P&R) coordinate with OPM, Department of State and the Office of the Director of National Intelligence to develop an overarching strategy for investigation of foreign national employees. The Army's investigative service provider, OPM, has limited authority to conduct background investigations on foreign nationals abroad. OPM will conduct a background investigation on a foreign national that resides in the United States long enough to establish investigative relevancy (typically three years). However, background investigations conducted by OPM on foreign nationals hired/employed abroad are restricted to the terms of the host nation agreement.

The G-2, in partnership with ASA(M&RA), is working to implement policy and procedures to enhance the accessions pre-screening process for certain categories of foreign nationals and United States persons with significant foreign loyalties and connections (i.e., Soldiers enlisting into Military Occupational Specialty (MOS) 09L Interpreter/Translator, MAVNI). Additionally, the Army has completed a comprehensive review of its contract linguist program. As a result, the Army developed and improved business processes and procedures related to the background vetting process. In addition, the G-2 is developing a comprehensive policy to implement additional screening measures and improve the background vetting of contract linguists and cultural role players. The G-2 will publish policies by 1 October 2010.

Key actions necessary to implement the recommendation include:

- (D) Adjustments to doctrine possibly required once policy and procedures are completed. Policy adjustments promulgated to meet the target date of 1 October 2010.
- (O) Preliminary working groups identify specific organizations best suited to execute updated policies and procedures.
- (T) The Army will identify specific training requirements once policy and procedures are completed.
- (M) The Army will fully implement the AIES for the efficient and effective processing of background investigations to the OPM. AIES is the Army's end-to-end enterprise approach for the centralized submission and quality review of background investigations submitted to OPM. AIES builds efficiencies into the background investigation submission process and has resulted in an 80% reduction in cycle time for the adjudication of security clearances and/or suitability determinations. The Army implemented eScreening capability as part of AIES, which reviews all background investigations completed by the OPM and submitted to the Army CCF. The eScreening review automatically identifies and highlights issues of security and CI concern for subsequent action. The Army has also established a Personnel Security Investigation Center of Excellence, which centralizes and conducts a quality review of all Army personnel security and suitability investigations prior to submission to OPM. The Army target for FOC of AIES is 4thnd Quarter FY11.
- (L) Once viable policies and procedures are completed, the Army recommends that the USD(I) coordinate with the ASA (M&RA), G-1, G-2 and G-3/5/7 to develop a strategy to disseminate and educate stakeholders regarding the enhanced security screening procedures and guidelines. In the interim, the G-2 will draft an Chief of Staff of the Army memorandum for Army senior leaders, apprising them of the Army's initiatives to address the system weaknesses in the security and suitability background vetting process. Target date for dissemination of this memo is July 2010.
- (P) Adjustments to personnel are required at the G-2 Linguist Support Office, AIES – Personnel Security Investigation Center of Excellence, INSCOM and TRADOC. Other personnel adjustments may be required once policy and procedures are implemented within DoD and the Army.

Resource Estimate ($ in Millions):

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
Security Screeners	41	Screen high risk populations						
Staff	17	Support						
Total	58		11.6	9.44	9.44	9.44	9.44	9.44

3) Finding 2.8 - DoDI 5240.6, *"CI Awareness, Briefing and Reporting Programs,"* does not thoroughly address emerging threats, including self-radicalization, which may contribute to an individual's potential to commit violence.

Recommendation 2.8 - (OTSG and OPMG in support) Update DoDI 5240.6 to provide specific guidance to the Services, combatant commands and appropriate agencies for CI aware-

ness of the full spectrum of threat information particularly as it applies to behavioral indicators that could identify self-radicalization.

Discussion - USD(I) drafted an updated version of DoDI 5240.6 and staffed it informally with the Services. They are currently revising the first draft based on the comments received from the informal staffing process. USD(I) expects to submit the draft for formal coordination in the immediate future. The Army is updating AR 381-12, "*Subversion and Espionage Directed Against the Army (SAEDA)*" re-titling it to "*Threat Awareness and Reporting*." The update includes additional observable indicators for espionage, terrorism and extremism and more robust reporting requirements, to include the activation of iSALUTE discussed in Chapter 4. OTJAG Administrative Law Division completed its review on 19 July 2010 and the publication is waiting for approval by the Army Publishing Directorate. Target date for publication of the updated AR 381-12 is 1 October 2010.

Following publication of AR 381-12, the G-2 and INSCOM will execute an expanded training and awareness program to build Army personnel awareness of the threat indicators and observable behaviors included in AR 381-12, their responsibility to report potential threats and the Army's reporting procedures.

Key actions necessary to implement the recommendation include:

- (D) The Army will adjust G-2 doctrine once it reviews the policy and procedures contained in DoDI 5240.6. The G-2 has released AR 381-12 to address the emerging threat in advance of the publication of DoDI 5240.6.
- (O) The G-2, working with INSCOM, has developed a concept plan that details the required personnel increase to the Army's CI organizations to execute the policy requirements of AR 381-12 and eventually, DoDI 5240.6.
- (T) The Army currently requires annual training in accordance with AR 381-12. Army needs to execute a long-term training strategy to improve the Army's Threat Awareness and Reporting program.
- (M) The G-2, working in conjunction with the G-6, developed and implemented a CI reporting link, titled iSALUTE on the AKO and AKO-S systems. Links for both systems are available to any Soldier or Civilian with an AKO or AKO-S account. When someone witnesses a suspicious activity, they can report it to Army CI via AKO or AKO-S. G-2 and CIO/G-6 staffs have addressed privacy and security concerns in the implementation plan. AKO link was operational as of 28 April 2010; AKO-S was operational 30 June 2010.
- (L) The G-2 will ensure that the public affairs office includes iSALUTE in the relevant strategic communications plan and is briefed to leadership across the Army.

Resource Estimate ($ in Millions):

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
CI Agents	14	Operations						
Instructors	2	Support						
Total	16		4	4	4	4	4	4

4) **Finding 2.14 - The DoD does not have a comprehensive and coordinated policy for CI activities in cyberspace. There are numerous DoD and interagency organizations and offices involved in defense cyber activities.**

Recommendation 2.14 - Publish policy to ensure timely CI collection, investigations and operations in cyberspace for identifying potential threats to DoD personnel, information and facilities.

Discussion: USD(I) drafted DoDI 5240.mm, "*Counterintelligence (CI) Activities in Cyberspace*" and staffed it formally to the Services. The Army has reviewed the first version, provided comments, met with the principal drafters of the DoDI and now is reviewing the second version. Army's comments and concerns were addressed by the USD(I) staff in this second version.

Key actions necessary to implement the recommendation include:

- (D) G-2 will evaluate the requirement for Army doctrine and policy when the DoD publishes Instruction 5240.mm, "*CI Activities in Cyberspace*."
- (O) G-2, working with INSCOM, has developed a concept plan that details the personnel and organizational structure required to execute CI activities in cyberspace. This concept plan is contained within the larger plan for the military intelligence rebalancing effort. The Army will adjust this concept plan if required due to publication of DoDI 5240.mm.
- (T) The highly technical nature of cyber CI and the velocity of technology development will require continued engagement to update the DIA's Joint CI Training Academy and the United States Army Military Intelligence Center at Fort Huachuca, Arizona.
- (M) Army will use existing computer hardware and software for current research and development of cyber training and education programs, while working to field new systems.
- (L) Work with INSCOM, Fort Huachuca, Joint Counter-Intelligence Training Academy and industry/academia to ensure the latest software applications are available for proper training CI agents and analysts.
- (P) Army currently receives National Intelligence Program funding for CI activities conducted in cyberspace.

5) **Finding 3.3 - The DoD's commitment to support JTTFs is inadequate.**

Recommendation 3.3.A - (OPMG in support) Identify a single point of contact for functional management of the DoD's commitment to the JTTF program.

Recommendation 3.3.B - (OPMG, US Army Criminal Investigation Command (CID) and OTJAG in support) Evaluate and revise, as appropriate, the governing memoranda of understanding between the FBI and different DoD entities involved with the JTTF to ensure consistent outcomes.

Recommendation 3.3.C - (CID in support) Review the commitment of resources to the JTTFs and align the commitment based on priorities and requirements.

Discussion- The ASD(HD & ASA), in coordination with USD(I), CI, was identified as the single DoD entity for developing requirements and associated program resourcing supporting the DoD's overall contribution to the JTTFs across the country. The current July 2009 Memorandum of Understanding (MOU) between the Federal Bureau of Investigation and DoD effectively articulates the purpose, mission, authorities, management, reporting and support arrangements necessary to ensure effective operational execution of the JTTF program. However, the increased emphasis on cooperation and information sharing along with increased DoD participation levels requires an updated MOU. The original MOU sat-

isfactorily addressed the Army's unique participation in the JTTFs which uses both Army CI Special Agents and Criminal Investigative Special Agents. G-2 will publish Army supplemental guidance once the FBI publishes the new MOU. USD(I) led the review of current DoD JTTF manning, reviewed prioritization based on threats and Service equities and deconflicted Service requests for additional JTTF authorizations. If resourced as proposed, DoD will eventually be represented in 85 of the 104 JTTFs across the country. The Army requested 17 additional CI agent positions and 9 CID investigator positions be added to the overall JTTF manning effort. Additionally, Army requested 8 CI agents for placement within FBI HQ activities. The FBI recommended this initiative and is intended to further integrate DoD into the FBI CT effort. USD(I) will forward the final manpower request OASD (HD & ASA) for submission to the Secretary of Defense this fall in time for the FY12 program submission.

Key actions necessary to implement the recommendation include:

- (D) The Army may make adjustments to doctrine once Army reviews the policy and procedures contained in the updated MOU. G-2 has updated AR 381-20, "*The Army Counterintelligence Program*," effective 25 Jun 2010, in order to address the unique role and responsibilities of Army CI agents filling JTTF positions. Army will reevaluate the need for implementing guidance memoranda when the DoD – FBI JTTF MOU is updated.
- (O) G-2, working with the INSCOM, has developed an implementation plan that details the positioning and functions for personnel increases expected in FY12 to the Army's overall JTTF contribution.
- (T) Increase the volume of DoD student throughput at the DIA Joint CI Training Academy and the DoJ Federal Law Enforcement Training Center to train individuals designated for assignment at JTTF related duties and positions.
- (L) G-2 will develop information pertaining to its continued participation in the FBI-lead JTTFs as a key element of the nation's CT effort. This point is critical for the larger strategic communications plan supporting the final report for the AIRT for the Fort Hood shooting.
- (P) Increase recruiting efforts of civilian CI agents to keep pace with increased operational requirements.

Resource Estimate ($ in Millions):

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
CI Agents	25	Operations						
CID Agents	9	Operations						
Total	34		5	5	5	5	5	5

D. Army G-3/5/7 Lead:

1) Finding 2.1 - DoD programs, policies, processes and procedures that address identification of indicators for violence are outdated, incomplete and fail to include key indicators of potentially violent behaviors.

Recommendation 2.1.A - (OTSG, G-1 and TRADOC in support) Update training and education programs to help DoD personnel identify contributing factors and behavioral indicators of potentially violent actors. The estimated date to initiate implementation efforts is October 2010 with completion during September 2011.

Recommendation 2.1.C - (G-1 and Army Safety Center in support) Develop a risk assessment tool for commanders, supervisors and professional support service providers to deter-

mine whether and when DoD personnel present risks for various types of violent behavior. The estimated date to initiate implementation efforts is October 2010 with completion in January 2012.

Discussion: Upon approval and funding of these recommendations, the G-3/5/7 will establish a working group to identify and assess existing training and education programs, research current doctrine and policy and determine if changes are necessary. The working group will consist of representatives from G-3/5/7, OTSG, TRADOC, Army G-1 and the Army Safety Center. Projected initial working group meetings will begin December 2010. The Army will develop a risk assessment tool to determine if personnel present risks for various types of violent behavior.

Key actions necessary to implement the recommendation include:

- (D) Discuss an accessible consolidated criminal investigation database or SAR system.
- (D) Address identification of violent behavior indicators, contributing factors, or prevention of workplace violence.
- (D) Write, staff, adjudicate and publish AR 525-XX, "*Protection*," and associated Department of the Army Pamphlet (DA PAM).
- (T) Modify existing or adopt new training requirements addressing behavioral observations and reporting.
- (M) Use existing computer hardware and software for research and development of training and education programs.
- (L) Work with INSCOM, OPMG and CID to ensure proper training of MPs and CID agents.
- (L) Work with TRADOC to develop a program of instruction that enables Soldiers to recognize behavioral characteristics or actions that could lead to or result in violent acts.

Resource Estimate ($ in thousands):

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
GS-14 or O-5	2	Research	284	330	0	0	0	0
GS-15/Step 5	1	Analysis	160	192	0	0	0	0
Training	2	Development	1,000	1,000	0	0	0	0
Total	5		1,444	1,522	0	0	0	0

Required personnel will:

- Research various FP training programs (threat identification, behavioral characteristics, interpretation, analysis, threat reporting, etc.).
- Seek advice on behavioral analysis of potentially violent actors.
- Make recommendations to modify existing programs or develop new training.
- Develop risk assessment tools.

2) **Finding 2.2 - Background checks on personnel entering the DoD workforce or gaining access to installations may be incomplete, too limited in scope, or not conducted at all.**

Recommendation 2.2.C - (OTSG, TRADOC, OPMG and G-2 in support) Educate commanders, supervisors and legal advisors on how to detect and act on potentially adverse behaviors that could pose internal threats. The estimated date to initiate implementation efforts is October 2010 with completion during October 2011.

Discussion: Upon approval and funding of this recommendation, the Army G-3/5/7 will establish a working group to identify and assess existing training and education programs, research current doctrine and policy and determine if changes are necessary. The working group will consist of representatives from G-3/5/7, OTSG, TRADOC, G-2 and OPMG. Projected initial working group meetings will begin December 2010. Required personnel, training resources and associated costs are:

Key actions necessary to implement the recommendation include:

- (D) Discuss an accessible consolidated criminal investigation database or SAR system.
- (D) Address identification of violent behavior indicators, contributing factors, or prevention of workplace violence.
- (D) Write, staff, adjudicate and publish AR 525-XX, "*Protection*," and associated DA PAM.
- (T) Modify existing or adopt new training requirements addressing behavioral observations and reporting.
- (M) Use existing computer hardware and software for research and development of training and education programs.
- (L) Work with INSCOM, OPMG CID to ensure proper training of MP and CID agents.
- (L) Work with TRADOC to develop a program of instruction for the soldier to enable him/her to observe behavioral characteristics or actions that could lead to or result in violent acts.

Resource Estimate ($ in thousands):

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
GS-14 or O-5	2	Research	284	330	0	0	0	0
GS-15/Step 5	1	Analysis	160	192	0	0	0	0
Training	2	Development	1,000	1,000	0	0	0	0
Total	5		1,444	1,522	0	0	0	0

Required personnel will:

- Research various FP training programs (threat identification, behavioral characteristics, interpretation, analysis, threat reporting, etc.).
- Seek advice on behavioral analysis of potentially violent actors.
- Make recommendations to modify existing programs or develop new training.
- Develop risk assessment tools.

3) **Finding 3.1 - The DoD has not issued an integrated FP policy. Senior DoD officials have issued DoD policy in several FP-related subject areas such as antiterrorism, but these policies are not well integrated.**

Recommendation 3.1.A - Assign a senior DoD official responsibility for integrating FP policy throughout the Department. The estimated date to initiate implementation efforts is September 2010 with completion in 2011.

Recommendation 3.1.B - (OTJAG, OGC, JTTFs, Joint Task Force National Capital Region Medical in support) Clarify geographic combatant commanders and military department responsibilities for FP. The estimated date to initiate implementation efforts is September 2010 with completion during October 2011.

Recommendation 3.1.C - (OTJAG in support) Review FP C2 relationships to ensure they are clear. The estimated date to initiate implementation efforts is September 2010 with completion in May 2012.

Discussion: To clarify FP C2 relationships, we must revise how we identify, prioritize, program, procure and sustain our protection enablers and align policy to achieve a safe work environment for our Soldiers, their families and our work force. Earlier in this report we identified a viable path forward for central procurement and sustainment for protection related equipment and have received support from ASA(ALT). Our current process does not provide Army leaders with visibility of protection program-related shortfalls and the opportunity to allocate resources to achieve an acceptable level of risk. In order to resolve this shortfall, the Army must implement the goals and objectives in the Secretary of the Army's directive 2008-02, "Army Protection." A single HQDA staff element for Protection, with the responsibility for all protection related functions, achieves unity of effort and establishes a sole focal point to synchronize all protection related functions including requirements determination, prioritization and programming.

The G-3/5/7 developed a detailed plan to establish a G-34 staff element to meet this requirement. See Appendix F for details. As outlined, the G-3/5/7 validates, prioritizes and identifies Army-wide protection requirements and submits the recommended path forward (e.g. priorities, programs and plans) to the SICE board. The SICE is the ideal body as it "uses an enterprise approach to provide fully integrated, efficient and effective services, facilities and infrastructure to Soldiers, families and civilians." Its responsibilities include resolving issues, synchronizing efforts and maturing initiatives. The SICE also provides a forum to adjudicate friction points in the path forward prior to presentation to the Senior Army Leadership for approval and inclusion in the Army Campaign Plan. The SICE is a forum for issues requiring General Officer/Senior Executive Service level review to ensure potential shortfalls and gaps are identified and resolved as part of the risk assessment process.

Additionally, since Major Objective 2-7, "Provide an Effective Protection Capability at Army Installations," is in the pre-decisional draft Army Campaign Plan dated 23 July 2010, we recommend the Army designate the G-3/5/7 as the lead. Furthermore, the Secretary of the Army should assign oversight to the VCSA who leverages Army Campaign Plan to track progress. Additionally, we recommend an annual review of the Protection function using the portfolio review process recently developed by the Army Staff.

4) **Finding 3.2 - DoD FP programs and policies are not focused on internal threats.**

Recommendation 3.2.A - (G-2 in support) Develop policy and procedures to integrate the currently disparate efforts to defend DoD resources and people against internal threats. The estimated date to initiate implementation efforts is September 2010 with completion in October 2011.

Recommendation 3.2.B - (G-2 and OPMG in support) Commission a multidisciplinary group to examine and evaluate existing threat assessment programs; examine other branches of government for successful programs and best practices to establish standards, training, reporting requirements/mechanisms and procedures for assessing predictive indicators related to possible violence. The estimated date to initiate implementation is September 2010 with completion in March 2012.

Recommendation 3.2.C - (G-2 and OPMG in support) Provide commanders with a multidisciplinary capability based on best practices such as the Navy's Threat Management Unit (NTMU), the Postal Service's "Going Postal Program" and Stanford University's workplace violence program. These programs can predict and prevent insider attacks. The estimated date to initiate implementation efforts is September 2010 with completion in March 2012.

Discussion: Upon approval and funding of these recommendations, the G-3/5/7 will complete and publish AR 525-XX, "*Protection*." The Army must accomplish the goals and objectives in the Secretary of the Army's directive 2008-02 as described in chapter 4 to integrate protection efforts. The Army will convene a multidiscipline working group with representatives from G-3/5/7, OPMG and G-2 to review the DSB recommendations on existing threat assessment programs. The initial meetings are projected to begin in December 2010. The Army will revise existing publications or directives to close gaps in policy and procedures.

Key actions necessary to implement the recommendation include:

- (D) Review existing publications.
- (D) Resolve conflicts and make recommendations pertaining to doctrine and regulations.
- (D) Develop an Army version of the NTMU.
- (O) Work within the approved protection construct as indicated in the discussion for recommendations 3.1 A-C.
- (O) Convene a working group to review DSB recommendations on effective Insider Threat prevention/mitigation programs.
- (O) Establish an ATMU to address internal threats.
- (T) Conduct an off-site training exercise for approximately 100 personnel and 2 conferences.
- (T) Adopt training requirements recommended by the NTMU and other federal, state or private organizations.
- (L) Once the ATMU and Army policy and doctrine are established, provide ATMU instruction at Army commander and Senior Leader training courses.

Required personnel, resources and associated costs are:

Resource Estimate ($ in thousands):

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
GS-14 or O-5	2	Research	284	330	0	0	0	0
Contractors	10	Analysis	4,305	3,055	0	0	0	0
Equipment and Training	1	Standup	60	75	0	0	0	0
Training Implementation	2	Training Development	1,000	1,000				
Total	15		5,649	4,460	0	0	0	0

Required personnel will:

- Research various FP programs and policies (threat reporting, interpretation, analysis, emergency response, asset integration, family assistance, etc.).
- Develop and coordinate recommendations for integrated FP efforts.
- Coordinate and submit regulations for publication.

5) **Finding 3.6 - There are no FP processes or procedures to share real-time event information among commands, installations and components.**

Recommendation 3.6.A - (G-2, CIO-G-6 and OPMG in support) Evaluate the requirement for creating systems, processes, policy and tools to share near real-time, unclassified FP information among all military installations to increase situational awareness and security response. The estimated date to initiate implementation efforts is September 2010 with completion in October 2012.

Discussion: Upon approval and funding of this recommendation, the G-3/5/7 will establish a working group to analyze and evaluate FP information, including its definition, collection, management, analysis and dissemination. Information reporting guidelines will be established with ARNORTH in CONUS and all ASCCs outside CONUS. The working group will review reports required by current DoDIs and ARs. Revising the *To*: and *Copy To*: lines of messages and emails will be an important part of this approach. Sharing information among all commands may be necessary based on the nature of the threat. The working group will consist of representatives from G-3/5/7, G-2, OPMG and CIO/G-6. The initial working group meetings are projected to begin in December 2010. Personnel necessary to implement the recommendation include two researchers for 6-12 months to identify reporting requirements.

Key actions necessary to implement the recommendation include:

- (D) Define "unclassified FP information".
- (D) Review AR 525-13, AR 525-27 other ARs, MEDCOM Orders, etc., that require reports be sent to higher/lower/adjacent/other headquarters.
- (D) Revise and reissue Execution Order: ARNORTH FY 2007 FP and Antiterrorism Responsibilities Execution Order, dated 05 December 2006.
- (P) Hire two (2) researchers for 6 months to identify required reports.

Personnel resources and associated costs are:

Resource Estimate ($ in thousands):

Type	Quantity	Purpose	FY11	FY12	FY13	FY14	FY15	FY16
Researcher	2	Research	275	350	0	0	0	0

Required personnel will:

- Analyze reporting requirements and methods.
- Make recommendations to streamline reporting requirements and information flow.

6) **Finding 4.1 - Services are not fully interoperable with all military and civilian EM stakeholders.**

Recommendation 4.1.A - (OPMG and ACSIM in support) Establish milestones for reaching full compliance with the IEM program. The target date to initiate implementation efforts of this recommendation is October 2011. The required implementation date per DoDI 6055.17 is 13 January 2014.

Recommendation 4.1.B - (ACSIM, US Army Forces Command, AMC and OPMG in support) Assess the potential for accelerating the timeline for compliance with the IEM program. The target date to initiate implementation efforts of this recommendation is October 2010. The required implementation date per DoDI 6055.17 is January 2014.

Discussion: DoD directed the Services to adopt procedures consistent with the NIMS and the NRF via DoD memoranda in 2004, 2005, 2007 and 2009. DoD formalized the DoD IEM Program with release of DoDI 6055.17 on 13 January 2009, including specific guidance on NIMS and NRF implementation. The Army established the EM Program as a formal program of record on 13 March 2009 with release of AR 525-27, "*Army Emergency Management Program*."

DoDI 6055.17 directs the Services to achieve IOC no later than 13 January 2011 and FOC no later than 13 January 2014. DoD IEM Program IOC requirements focus on initial actions to field and use installation emergency managers at all DoD installations. The Installation Emergency Manager serves as the principal advisor and action officer supporting the installation commander in developing and executing the IEM Program across all five phases of the EM cycle: Preparedness, Mitigation, Prevention, Response and Recovery. The Installation Emergency Manager is the lead action officer in:

- Establishing IEM Working Groups (EMWG) at the installation level.
- Leading the EMWG in conducting a comprehensive Risk Management process to identify all natural, technological and terrorism hazards impacting the installation and the relative risk associated with each identified hazard.
- Leading the EMWG in developing a comprehensive, integrated IEM Plan, in order to implement NIMS, support the NRF and integrate previously disparate single-hazard plans and procedures into a synchronized effort by the Installation.

DoD IEM Program FOC requirements include organizing, training, equipping, exercising and sustaining all the program capabilities identified within DoDI 6055.17, including MWN systems (see Recommendation 4.4), Installation EOCs (see Recommendation 4.5) and Support Agreements (see Recommendation 4.7).

Developing program of record capabilities required by the DoD IEM Program FOC targets is a multi-year effort requiring the organization, manning, training, equipping and exercising of multiple capabilities across response and recovery operations resulting from all hazards. The program of record, conducted by ASA(ALT), includes establishing a baseline of an installation's current on-hand capabilities and encompassing a complete life-cycle-management process.

A key element to accelerating this timeline is fielding trained and qualified Installation Emergency Managers at all installations in order to initiate the emergency planning process and the development of supporting capabilities for program execution. Based on current manpower authorizations and budget constraints associated with the Army EM Program's (High) Visibility Installation Protection Program (VIPP) MDEP, acceleration of program implementation is not possible without additional manpower, training and exercise funding. Comprehensive policy on implementation requirements is under development in the draft DA PAM 525-XX, "Army Emergency Management Program," instruction.

The Army utilizes its existing Emergency Management Steering Group (EMSG) chaired by G-3/5/7 to communicate IOC and FOC targets and implements the Army EM Program across all HQDA, ACOM, ASCC and DRU stakeholders. The Army uses its EM Workshop to promulgate implementation guidance, conduct required training and assist installation-level implementation efforts. Service Area 604 (Army Emergency Management) Installation Status Report is used to gauge implementation status, installation readiness and implementation cost drivers. It also uses existing membership of the Army EMSG, specifically G-3/5/7 and IMCOM, to revise outdated Service Area 75 (Army Emergency Management Services) Common Levels of Support criteria, ensuring optimal use of limited resources to implement the program of record.

Key actions necessary to implement the recommendation include:

- (D) Revise AR 525-27, "Army Emergency Management Program," approve Draft DA PAM 525-XX and support supplements to DA-PAM 525-XX from ACOMs, ASCCs and DRUs.
- (D) Develop and Maintain an IEM plan at each installation.
- (D) Develop an FM for EM operations.
- (D) Complete TRADOC DOTMLPF Integration Analysis (in progress).
- (O) Participate in DoD EMSG (in progress), establish Army EMSG (complete) and establish IEM Working Groups.
- (O) Identify Higher Headquarters EM Program Coordinators, Installation Public Health Emergency Officers, Installation EOC Staff, Response Teams, Mass Care Teams, Evacuation Management Teams and Recovery Teams.
- (T) Conduct NIMS phase 1 and phase 4 training.
- (T) Develop and implement Army EM Course (new training at Army Management Staff College), implement draft multi-year training plan for emergency managers and supporting functional areas.
- (T) Develop and implement EM exercise requirements including the Installation FP Exercise (IFPEX) series (in progress).

- (M) Field and sustain E911 system, MWN systems and COP systems at the installation level (see Recommendations 4.2, 4.4 and 4.5).
- (L) Provide EM education within existing General Officer/Senior Commander Course, Garrison Pre-Command Course, Garrison Sergeant Major Course, Director of Plans, Training and Mobilization Training Course and Regional Installation Support Team Course at Army Management Staff College (in progress).
- (P) Field and maintain G-3/5/7 emergency manager and supporting staff.
- (P) Field and maintain installation emergency managers at all installations (in addition to 54 existing positions).
- (F) Develop, coordinate and sustain consolidated dispatch centers and installation EOCs (see Recommendations 4.2 and 4.5).
- (F) Coordination with support agencies to provide and maintain support facilities.

Upon approval and funding of recommendations, the Army will field and train an additional 196 Installation Emergency Managers in addition to the existing 54 authorized positions in the FY 2010 budget. Fielding costs represent the full loaded cost of 196 additional positions across Army installations worldwide. Identify training costs for initial training and supporting train-the-trainer courses for identified response, mass care, evacuation management and recovery teams supporting EM requirements.

Resource Estimate ($ in Millions)

Type	FY11	FY12	FY13	FY14	FY15	FY16
Emergency Managers (196 positions)	0	5.63	5.63	5.63	0	0
Emergency Manager Sustainment	0	0	6.03	6.03	6.03	6.03
Mobile Training Teams (MTTs)	0	1.83	1.83	1.83	0	0
MTT Sustainment	0	0	2.33	2.33	2.33	2.33
Train the Trainer Teams (TTTs)	0	.56	.56	.56	0	0
TTT Sustainment	0	0	.76	.76	.76	.76
Total	0	8.02	17.14	17.14	9.12	9.12

7) Finding 4.2 - There is no DoD policy implementing public law for a 911 capability on DoD installations. Failure to implement policy will deny the military community the same level of emergency response as those communities off base.

Recommendation 4.2.A - (ACSIM and OPMG in support) Develop policy that provides implementation guidance for E911 services in accordance with applicable laws. The target implementation date for this recommendation is 31 January 2016.

Discussion: Public Laws 106-81 (Wireless Communications and Public Safety Act of 1999), 108-494 (Enhance 911 Act of 2004) and 110-283 (Net 911 Improvement Act of 2008) establish requirements for fielding and using E911 reporting and dispatch capabilities within the United States. E911 provides the capability for dispatch center operators to automatically receive and use the telephone number and address of the caller to decrease emergency response times for data collection at the dispatch center and information transfer to first responders.

E911 requires a well managed telecommunications infrastructure database capable of providing ANI and ALI information. A GIS enabled CAD terminal receives this information. E911 provides ANI/ALI information, speeding the call-taking process and automatically identifying the closest available first responder units based upon station locations and GPS location updates from these units resulting in decreased response times and more efficient use of response assets.

Dispatch procedures are ineffective due to legacy telecommunications infrastructure on Army installations including the use of multiple conventional seven digit emergency numbers (varying by installation), the presence of multiple agency dispatch centers on a single installation, lack of supporting technology at existing dispatch centers and the dependence upon untrained and/or uncertified borrowed military and civilian manpower for staffing.

The Army will establish an E911 Working Group consisting of G-3/5/7 Protection Division, ACSIM/IMCOM (Fire & Emergency Services, Law Enforcement, Physical Security and Public Works representatives), AMC, OPMG, OTSG and TRADOC no later than July 2011. The working group will determine Army standards and requirements for E911 capabilities to include acquisition, fielding and sustaining strategies.

Key actions necessary to implement the recommendation include:

- (D) Revise AR 420-1, "*Army Facilities Management*" and AR 190-13, "*The Army Physical Security Program.*"
- (D) Consolidate dispatch capabilities between organizations on bases (Fire & Emergency Services, Law Enforcement, Physical Security, Medical, Public Works, etc.).
- (O) Identify manpower usage for existing dispatch centers at the installation level to identify potential manpower realignment, manpower gaps and training needs.
- (O) AR 420-1 requires trained and certified DoD Telecommunicators for dispatch operations.
- (T) Identify DoD Telecommunicator I/II training requirements, identify E911 initial and recurring training requirements. Incorporate E911 requirements into all EM and Protection exercise requirements including the IFPEX Series.
- (M) Field and sustain new E911 consoles and Mobile Data Terminals for response units and trunked radio systems.
- (M) Develop and maintain GIS map data, maintain/upgrade and map telephone switches (PBX), Link E911 system to landline providers, cellular providers, Voice over Internet Protocol services and Defense Switched Network.
- (F) Develop, field and sustain consolidated dispatch centers to perform dispatch operations for all response and recovery agencies (can be co-located with an installation EOC). Develop and sustain supporting dispatch center infrastructure (servers, heating, ventilating and air conditioning system, primary and alternate power, radio networks, etc.).

Upon approval and funding of recommendations, the Army fields and trains dispatch personnel, fields E911 consoles and CAD systems at 105 domestic installations.

Personnel resources and associated costs are:

Resource Estimate ($ in Millions):

Type	FY11	FY12	FY13	FY14	FY15	FY16
E 911 Phone consoles	0	28	28	28	0	0
E 911 Consoles sustainment	0	2.6	2.6	2.6	2.6	2.6
Computer Aided Dispatch (CAD) System	0	7	7	7	0	0
Type	**FY11**	**FY12**	**FY13**	**FY14**	**FY15**	**FY16**
CAD Sustainment	0	0	.7	.7	.7	.7
Manpower (Dispatchers) (1260 positions)	0	36.33	36.33	36.33	0	0
Dispatcher Sustainment	0	0	39.33	39.33	39.33	39.33
Total	0	73.93	113.96	113.96	42.63	42.63

8) Finding 4.4 - Based on JS Integrated Vulnerability Assessments, many DOD installations lack mass notification capabilities.

Recommendation 4.4.A - (ACSIM and G-8 in support) Examine the feasibility of advancing the procurement and deployment of state-of-the-art mass warning systems and incorporate these technologies into emergency response plans. Target date to initiate implementation of this recommendation is 1 October 2011. Target implementation date for this recommendation is 31 January 2014.

Discussion: MWN system capabilities are a core component of the DoD IEM Program (DoDI 6055.17 Enclosure 6), enabling commands to quickly and effectively warn the installation populace of an existing and impending emergency and direct protective actions before, during and after an incident. MWN system capabilities consist of an interdependent network of external speakers (Giant Voice), internal building notification systems, Telephone Alerting Systems, Computer-based Notification Systems and existing civilian-provided over-the-air Emergency Alert System for radio and television networks and use of existing technologies, such as emergency vehicle loudspeaker broadcasts, per Unified Facilities Criteria 4-021-01.

Current capabilities are a mix of different systems and providers with no standard resource sponsor, system configuration, message content, or system control process. The JS Integrated Vulnerability Assessment process documented these deficiencies based upon the MWN system requirements specified in DoDI 2000.16 (Enclosure 3, Standard 21) and DoDI 6055.17 (Enclosure 6). The Army conducted MWN system surveys in August 2009 and January-March 2010, identifying current capabilities at the installation level. No identified resource sponsor exists for MWN system capabilities with the majority of installations funding these capabilities through end-of-the-year money or from resources provided by the JS's Combating Terrorism Readiness Initiative Fund, providing fielding resources only with no sustainment funding. There are no existing MDEP-validated critical requirements and associated critical funding for fielding or sustainment of MWN systems, with the limited exception of the Army EM Program's (High) VIPP MDEP sustainment of critical mission MWN systems fielded Joint Program Manager-Installation Protection Program as described above.

The Army will establish a MWN Working Group consisting of G-3/5/7 Protection Division, Installation Program Evaluation Group (II PEG), ACSIM/IMCOM (Fire & Emergency Services, Antiterrorism, Physical Security and Public Works representatives), Military Construction (MILCON) representatives, Network Enterprise Center representatives, AMC, OTSG and

OPMG no later than July 2011. The Army MWN Working Group gathers MWN information on all Army installations and their current systems and capabilities to identify gaps and best practices. The working group determines Army standards and requirements for MWN capabilities, identifies processes for acquisition, fielding and sustainment at the installation level and identifies processes for fielding and sustaining supporting infrastructure.

Key actions necessary to implement the recommendation include:

- (D) Revise DoDI 6055.17 (in progress), revise AR 525-27, revise AR 420-1 regarding Fire & Emergency Services dispatch operations, AR 190 series (-156/-13/-16) regarding law enforcement and physical security dispatch operations, approve draft DA PAM 525-xx and address telecommunications and IT policy requirements related to fielding of specific MWN elements.
- (D) Include MWN tactics, techniques and procedures within the proposed FM for EM operations.
- (O) Align MWN system control to dispatch centers and installation EOCs.
- (T) Identify initial and recurring training requirements for fielded MWN systems, incorporate MWN training requirements into ongoing TRADOC DOTMLPF analysis and incorporate MWN requirements into all EM and Protection exercise requirements including the IFPEX Series.
- (M) Field and sustain MWN systems, augmenting existing systems when feasible and fielding complete systems when necessary.
- (L) Participate in senior leader education through existing Army Management Staff College courses (see Recommendation 4.1 discussion).
- (F) Field and sustain external speaker (Giant Voice) towers and supporting infrastructure.

Recommend consolidation of MWN system requirements under the Army EM Program's (High) VIPP MDEP. Comprehensive policy on these requirements is under development in the draft DA PAM 525-XX Army EM program instruction.

Upon approval and funding, the Army fields and sustains standardized MWN system capabilities at installations worldwide. Costs for Interior Building Notification System fielding can be off-set by existing MILCON budget.

Resource Estimate ($ in Millions):

Type	FY11	FY12	FY13	FY14	FY15	FY16
Giant Voice	0	26.96	26.96	26.96		
Giant Voice Sustainment	0	0	2.6	2.6	2.6	2.6
Indoor Voice	0	67	67	67		
Indoor Voice Sustainment	0	0	8.03	8.03	8.03	8.03
Telephone Alert System	0	6.4	6.4	6.4		
TAS Sustainment	0	0	0.63	0.63	0.63	0.63
Software Alert Systems	0	5.43	5.43	5.43		
Software Sustainment	0	0	0.53	0.53	0.53	0.53
Total	0	105.79	117.58	117.58	11.79	11.79

9) **Finding 4.5 - Services have not widely deployed or integrated a COP capability into Installation EOCs per DoD direction.**

Recommendation 4.5.A - (ACSIM, G-2 and CIO/G-6 in support) Examine the feasibility of accelerating the deployment of a state-of-the-art COP to support installation EOCs. Target date to initiate implementation of this recommendation is 01 October 2011. Target implementation date for this recommendation is 31 January 2014.

Discussion: The COP capability is a core component of the DoD IEM Program (DoDI 6055.17 Enclosure 6), enabling commands to quickly and effectively exchange information, resource requests and coordinate response and recovery operations with civil and military partners. The COP consists of a GIS enabled Incident Management System, based upon the Emergency Data Exchange Language and Common Alerting Protocol standards, used within the installation EOC. Common standards within the COP system allow user to interface with civil and military partners using other proprietary software systems through the Department of Homeland Security's Disaster Management – Open Platform for Emergency Networks. These common standards also allow the COP to communicate with the HAZCOLLECT system to develop and release Non-Weather Emergency Messages through the Emergency Alert System, a key component of the MWN system capabilities identified in Recommendation 4.4.

Current capabilities include a mix of different civilian and military proprietary software systems and a selection of manual and software mapping applications. The larger associated issue is the lack of common standards and resource sponsor for fielding, staffing, training, equipping, exercising and sustaining installation EOCs as required by the FOC goals identified within the DoD IEM Program (DoDI 6055.17). These deficiencies are documented by the Joint Staff Integrated Vulnerability Assessment process based upon the COP requirements specified in DoD Handbook 0-2000.12-H and DoDI 6055.17 (in Enclosure 6). No existing MDEP has validated critical requirements and associated critical funding for fielding or sustainment of COP systems or the supporting Installation EOC capabilities.

The Army will establish a COP Working Group consisting of G-3/5/7 Protection Division, II PEG, ACSIM/IMCOM (Fire & Emergency Services and Antiterrorism representatives), Network Enterprise Center representatives, AMC, OTSG and OPMG no later than July 2011. The Army COP Working Group will gather COP and supporting installation EOC information on all Army installations concerning current systems, capabilities and limitations in relation to existing standards to identify gaps and best practices. The working group will determine Army standards and requirements for COP systems and supporting EOCs, identify processes for acquisition, fielding and sustainment of COP systems at the installation level and identify processes for fielding and sustaining supporting infrastructure, including development of Installation EOCs, organization, training and exercising of EOC staff and GIS requirements.

Key actions necessary to implement the recommendation include:

- (D) Revise DoDI 6055.17 (in progress), AR 525-27, Approve Draft DA PAM 525-XX, address telecommunications and IT policy requirements related to fielding of specific COP elements (GIS, Incident Management System, Modeling Programs, etc.).
- (D) Include COP and EOC tactics, techniques and procedures within the proposed field manual for EM operations.
- (O) Define the requirements for the Installation EOC staff, including roles, responsibili-

ties, standard operating procedures and relationship between the senior commander and installation commanders during emergencies (to reduce duplication of effort and proper application of capabilities at the installation level) (in progress within draft DA PAM 525-xx).

- (T) Identify initial and recurring training requirements for COP and supporting EOC capabilities, to include EOC Mobile Training Course.
- (M) Field and sustain COP systems-to include Incident Management System, GIS system, Hazard Modeling systems, field and sustain EOC equipment (computers, projectors, printers, servers and telecommunications).
- (L) Participate in Senior Leader education through existing Army Management Staff College courses (see Recommendation 4.1 discussion) and incorporate COP and EOC requirements into all EM and Protection exercise requirements including the IFPEX Series.
- (P) Field and sustain the position of EOC Coordinator and GIS Coordinator (for COP & E911 systems), use contract or Civilian manpower for the Mobile Training Team and Train the Trainer Teams.
- (F) Develop dedicated or shared EOC facilities and field/sustain supporting EOC infrastructure.

We recommend that the COP and supporting Installation EOC requirements be identified as a key element of the ongoing TRADOC-led DOTMLPF analysis effort for the Army EM Program. Comprehensive policy on these requirements is already under development in the draft DA PAM 525-XX, "Army Emergency Management Program," instruction.

Upon approval and funding of recommendations, the Army fields and sustains standardized COP capabilities at installations worldwide.

Resources and associated costs are:

Resource Estimate ($ in Millions):

Type	FY 11	FY 12	FY 13	FY 14	FY 15	FY16
Common Operating Picture System	0	7	7	7	0	0
Sustainment Costs	0		2.23	2.23	2.23	2.23
Total	0	7	9.23	9.23	2.23	2.23

10) Findings 4.5 - Services have not widely deployed or integrate a COP capability into Installation EOCs per DoD direction.

Recommendation 4.5.B - (ACSIM, G-2 and CIO/G-6) Develop an operational approach that raises the FPCON in response to a scenario appropriately and returns to normal while considering both the nature of the threat and the implications for force recovery and healthcare readiness in the aftermath of the incident.

Discussion: The target date to initiate implementation of this recommendation is 01 October 2011. The required implementation date per DoDI 6055.17 is 13 January 2014. During research into this recommendation, it was determined installation commanders and senior commanders have both the authority and the training for procedures in raising and lowering FP conditions at their installation. No cost estimate necessary.

11) Finding 4.6 - Stakeholders in the DOD IEM program have not synchronized applicable programs, policies, processes, procedures; Better synchronization and coordination would remove redundant planning, ID policy seems, focus programmed resources and streamline procedures in IEM.

Recommendation 4.6.A - (OPMG and ACOMS in support) Review responsibilities for synchronizing OSD/Army programs, policies and procedures related to IEM.

Recommendation 4.6.B - (OPMG and ACOMS in support) Establish policy requiring internal synchronizing of installation programs, plans and response for EM.

Discussion: Target date to initiate implementation of these recommendations is 01 October 2011. The required implementation date per DoDI 6055.17 is 31 January 2014. The release of the DoD IEM Program (DoDI 6055.17) and the Army EM Program (AR 525-27) are initial steps to policy synchronization regarding the Army's ability to prepare for, mitigate, prevent, respond to and recover from all natural, technological and terrorism hazards impacting the Army's missions, communities and infrastructure. The primary role of IEM is to synchronize, coordinate and integrate the Installation's comprehensive response to and recovery from emergencies involving multiple agencies and/or multiple jurisdictions. These response and recovery capabilities include such disparate programs as Fire & Emergency Services, Public Works, Antiterrorism, Physical Security, Logistics, Medical, Public Health, Information Systems, Transportation, Morale Welfare and Recreation (MWR), ACS and Housing Services, which are all managed by separate and uncoordinated policy and resource sponsors. Each supporting programs require additional DOTMLPF requirements in order to support implementation of the DoD IEM Program (DoDI 6055.17) FOC goals identified in Recommendation 4.1.

The release of the Army Protection Directive 2008-02 and the development of the Army Protection (AR 525-XX) regulation consolidate the Protection mission to encompass all natural, technological and terrorism hazards and directed a comprehensive approach to managing the Army's preparedness for, response to, and recovery from these hazards. Revisions to supporting Army policy for all functional areas identified by the Army Protection regulation, to include those identified by the Army EM Program, will require review and possible revision to ensure the supporting architecture and capabilities exist to support the mission.

No cost estimate is necessary to implement this recommendation. The supporting policy is already established under Secretary of the Army and Chief of Staff of the Army signature authorities.

12) Finding 4.7 - MAAs between DOD and civilian support agencies across the Services are not current.

Recommendation 4.7.A - (ACSIM in support) Review IEM programs ensuring correct guidance on integrating, tracking, exercising and inspections of MAAs.

Discussion: Target date to initiate implementation of recommendation is October 2011. Estimated completion date is January 2014. Support Agreements, including MAAs, MOUs, Memoranda of Agreement, Inter-Service Support Agreements and Support Contracts are a key element of coordinating response and recovery operations with civil and military partners. The DoD IEM Program and Army EM Program (AR 525-27) directs the development, approval, maintenance and exercising of support agreements. Both DoD and Army policy are under revision; update and clarification of support agreement responsibilities and procedures and de-confliction between disparate policy requirements within policies governing Security, Law Enforcement, Fire and Emergency Services, Medical and Public Works is ongoing. No cost estimate necessary to implement the recommendation. The Secretary of the Army and Chief of Staff of the Army signature authorities establish support policy. The DoD IEM Program (DoDI

6055.17) requires annual exercise of all EM capabilities, including support agreements (see DoDI 6055.17 Enclosure 5), to validate effectiveness of these agreements. The Army EM Program (High) VIPP MDEP identifies cost for this exercise component. The Fort Hood AIRT recommends identification of support agreement requirements as key elements in the ongoing TRADOC-led DOTMLPF analysis for the Army EM Program. Comprehensive policy on these requirements has been developed in the draft DA PAM 525-XX Army EM Program instruction.

E. OPMG Lead:

1) **Finding 2.1 - DoD programs, policies, processes and procedures that address identification of indicators for violence are outdated, incomplete and fail to include key indicators of potentially violent behaviors.**

Recommendation 2.1.B - (G-3/5/7 and OTSG in support) Coordinate with the FBI's Behavioral Science Unit's Military Violence unit to identify behavioral indicators that are specific to DoD personnel. **(Note: This recommendation requires OSD action before the Army can implement)**

Discussion: CID coordinated with the FBI's Behavioral Science Unit and determined that there are no behavioral indicators specific to DoD personnel. CID participates in the Comprehensive Analysis of Military Offenders study of behavioral indicators specific to DoD personnel. This research project includes military, government and academic stakeholders on intra-military violence. The proposal submitted to DoD explained that the Comprehensive Analysis of Military Offenders will build a platform between military investigative analysis, academic support and perpetrator-motivated behavioral perspectives by examining military offender motivations. The three (3) long-range actions for this study are:

- Conduct interviews of military offenders to elicit their values, beliefs and paradigms.
- Identify motives for committing acts of interpersonal violence.
- Utilize retrieved data to develop vetted training and consultative deliverables designed to improve mitigation and prevention, preparedness, response and recovery measures relating to acts of interpersonal violence that enhance and exceed current practices.

Upon receipt of information from either the DSB effort or the OPMG/CID effort with the FBI Behavioral Science Unit, the OPMG will forward supporting tasks to ASA(M&RA)/G-1 to implement recommendation 2.1.D.

2) **Finding 2.11.A - DoD guidance on establishing information sharing agreements with federal, state and local law enforcement and criminal investigation organizations does not mandate action or provide clear standards.**

Recommendation 2.11.A - (OTJAG in support) Require the Military Departments and Defense Agencies to establish formal information sharing agreements with allied and partner agencies; federal, state and local law enforcement; and criminal investigation agencies, which clearly establishes standards regarding scope and timeliness. **(Note: This recommendation requires OSD action before the Army can implement)**

Discussion: The Army OPMG will identify best practices as a model for agreements with Federal, State and local law enforcement and criminal investigation organizations that would mandate action and provide clear standards.

USD(I) currently chairs a multi-Service, multi-division working group to coordinate and negotiate with the Department of Justice and the FBI to rewrite the Department of Justice-DoD Memorandum of Agreement that covers information sharing in general, and more

specifically, information sharing between the FBI's JTTFs. The goal is to have the memorandum of agreement completed in FY 2011. The Services will include manning of JTTFs by the affected divisions within the memorandum of agreement.

CID has ten approved positions on its Table of Distribution and Allowances for positions on JTTFs, but these positions are unfunded. This relates to finding 3.3.C.

The Army recommends the DoD and Department of Justice review current information sharing policies with desired end state of improving cooperation and coordination. Most federal, state and local law enforcement agencies tend to follow the FBI lead in regard to information sharing. Historically, the FBI independently decides when to release control of information and share it with outside agencies. In turn, any other federal, state and local agency that acquires information through their own investigations release information when they want to. An agreement between all levels of law enforcement would facilitate improved relations at the state and local levels.

Key action necessary to implement the recommendation includes:

- (P) Policy revisions in response to information sharing memoranda of agreement should be anticipated. If each memorandum of agreement is unique, specific policy adjustments may be required. Currently the originating agency is responsible to specify information release parameters; military law enforcement offices will establish Memorandums of Agreement/ Memorandums of Understanding at installation level to facilitate information sharing.

Resource Estimate ($ in Millions):

Type	Quantity	FY11	FY12	FY13	FY14	FY15	FY16
JTTF Positions	10	0	1.5	1.5	1.5	1.5	1.5

3) **Finding 3.4.A. - There is no formal guidance standardizing how to share FP threat information across the Services or the Combatant Commands.**

Recommendation 3.4.A - (G-2 and CID in support) Direct the development of standard guidance regarding how the military criminal investigative organizations and CI organizations will inform the operational chain of command. **(Note: This recommendation requires OSD action before the Army can implement)**

Discussion: OPMG will work with the G-2 and CID on future DoD policy and procedure development forums. The DoD proponent for FP will lead a working group consisting of the Services and other DoD Components to develop and implement DoD policy for sharing threat information by 31 October 2010. The task milestones and completion suspense of the DoD working group are:

- 31 July 2010- DoD components identify FP threat information requirements to DoD FP proponent
- 31 July 2010- Identification of DoD FP principal staff agent
- 31 October 2010- DoD FP proponent establishes policy and processes for sharing FP threat information between Combatant Commands, Services, Defense intelligence agencies and Defense Criminal Investigative and Defense CI organizations
- January 2011- DoD update of AT, FP, CI, intelligence and law enforcement policies, procedures and training

- June 2011- DoD FP proponent and USD(I) conduct an evaluation of effectiveness of implemented DoD policies

An informal DoD working group identified multiple organizations where the fusion, exchange and dissemination of FP threat information occur. Services have established fusion cells: the Army's CI Law Enforcement Center and Antiterrorism Operations Intelligence Cells, the Navy's Multiple Threat Alert Center and the Air Force's Investigative Collection Operations Nexus. All analyze and fuse FP and threat information and disseminate it within their Services. Although these Service fusion cells share relevant information with other Services, there is no written DoD policy governing the dissemination across the DoD for FP threat information. As a result, there are gaps in information sharing.

OPMG and the G-2 will participate and contribute to the DoD working group and will identify any changes that are required to Army policies or procedures. Changes to Army policies or procedures are not likely to occur until the DoD policies are established in January 2011.

Key actions necessary to implement the recommendation include:

- (P) Revision of CID and CI policy will likely be required when the DoD revises its policy.
- (D, T, L) Develop a strategic communication plan for each task if necessary; once viable policies and procedures are identified, OPMG will coordinate with G-2 and CID to develop a strategy to share and disseminate FP threat information consistent with law and ARs.
- (D) Revise AR 195-2, "*Criminal Investigations Activities*," as it assigns primary responsibility to operate a criminal intelligence program, to include obtaining, recording, processing, analyzing and disseminating information concerning criminal activities and terrorist threats to CID and information sharing with Army CI (para 1-7, i. and k.)
- (D) Revise AR 381-20, "*Army Counterintelligence Program*," as it regulates CI collection and reporting procedures, to include sharing information developed from CI investigations with effected commands (Para. 6-3)
- (D) Revise AR 525-13, "*Antiterrorism*," which directs all ACOMs to collect, analyze and disseminate terrorism threat information. (Para. 4-3)

4) Finding 3.5 - The DoD does not have direct access to a FP threat reporting system for suspicious incident activity reports.

Recommendation 3.5.A - (G-2 in support) Appoint a single Executive Agent to implement, manage and oversee this FP threat reporting system. (Note: This recommendation requires OSD action before the Army can implement)

Recommendation 3.5.B - (G-2 in support) Appoint a single Executive Agent to implement, manage and oversee this FP threat reporting system.

Discussion: On 20 May 2010, the Secretary of Defense directed the implementation of eGuardian as the DoD Law Enforcement SAR system. The ASD(HD&ASA) is the DoD lead for eGuardian and has drafted a Directive Type Memorandum to disseminate policy and procedures for eGuardian use. The Directive Type Memorandum is expected to be published by 30 July 2010. The Army Provost Marshal General will serve as the Department of the Army proponent for eGuardian policy and CID will serve as the Army eGuardian program manager. CID has developed a phased implementation plan and is currently staffing an

implementation CBA. OPMG/CID will ensure that information from eGuardian is shared with G-2/CI as appropriate and when authorized by law. Future funding portrayed in the CBA for the 81 analysts and program management personnel through FY 2012 is $19.8M. OSD is considering a Lead Service rather than an Executive Agent for eGuardian.

Public perception of the U.S. military spying on Americans led to the cancellation of the Threat and Location Observation Notice (TALON) SAR system in August 2007 and privacy concerns are items of congressional interest. The FBI and DoD have established several mechanisms to preserve individual privacy, including access to eGuardian being limited to law enforcement personnel and agencies. As the program owner, the FBI has the lead in ensuring privacy issues are adequately addressed.

Key actions necessary to implement the recommendation include:

- (P) OPMG has worked with the Army G-2 and CID to draft Army policy. Formal staffing of the Army policy will take place upon publication of OSD Directive Type Memorandum. Once the eGuardian Directive Type Memorandum is published, OPMG will finalize the draft Army policy and publish by November 2010.
- (D) CID is developing a phased implementation plan which will start in November 2010 and be completed by February 2012.
- (M) In order to adequately analyze and input SAR system information, CID requires funding for 81 criminal analysts and program management personnel.
- (O) Preliminary working groups have identified specific organizations that are best suited to execute information sharing tasks. When policy and procedures are identified within the DoD working group, adjustments to current organizational structures may be required.

Resource Estimate ($ in Millions):

Type	Quantity	FY 11	FY 12	FY 13	FY 14	FY 15	FY16
Information analysts and program management personnel	81	0	19.8	19.8	19.8	19.8	19.8

5) **Finding 3.7 - DoD installation access control systems and processes do not incorporate behavioral screening strategies and capabilities and are not configured to detect an insider threat.**

Recommendation 3.7.A - (G-2 in support) Review best practices for adoption, including outside the U.S. Government, to determine whether elements of access control systems and processes to help detect insider threats. **(Note: This recommendation requires OSD action before the Army can implement)**

Recommendation 3.7.B - (G-2 in support) Review and adopt leading edge tools and technologies [behavior screening capabilities to detect an insider threat] that augment physical inspection for protecting the force. **(Note: This recommendation requires OSD action before the Army can implement)**

Discussion: The Army OPMG will work to identify technologies and best practices to detect insider threats in coordination with other Services through the DoD Physical Security Equipment

Action Group's Defense Installation Access Control Working Group. The Defense Installation Access Control Working Group enhances and standardizes access control procedures throughout the DoD to achieve a DoD-wide and federally interoperable access control capability.

The DoD Physical Security Equipment Action Group funded a $250,000 study in January 2010 that tasked the Defense Installation Access Control Working Group to conduct an Insider Threat Behavioral Analysis Study. This study focuses on how behavior pattern recognition screening procedures and technologies employed at entry control points, pedestrian gates, visitor centers and/or other customer service locations can detect a person under unusual stress with the potential intent to do harm. The Insider Threat Behavioral Analysis Study runs from 1 May 2010 – 31 October 2010 and will:

- Identify technologies available to detect behavioral patterns that detect unusual stress with the potential intent to do harm.
- Identify training available to detect behavioral patterns that detect high stress or potential intent to do harm.
- Identify procedures and checklists available that may aid members in the DoD to detect a person under stress with the potential intent to do harm.

The Defense Installation Access Control Working Group will also interview SMEs in the DoD, Federal & Civilian Agencies and academia to identify best practices. Once identified as best practices and adopted, they would be part of annual external evaluations of security forces conduct of access control procedures (in accordance with AR 190-13, "Army Physical Security Program").

OPMG will review the results of the Insider Threat Behavioral Analysis Study and identify any best practices appropriate for adoption by 30 November 2010.

OPMG will coordinate viable best practices with the OTJAG and IMCOM to develop a strategy to communicate to installations how best practices will be used to screen for insider threats consistent with law and ARs.

Key actions necessary to implement the recommendation include:

- (D) Best practices identified by the Defense Installation Access Control Working Group may require policy adjustments.
- (D) Best practices identified by the Defense Installation Access Control Working Group may require doctrinal adjustments.
- (T) TRADOC should develop a behavioral indicator TSP to train military police, civilian police and security guards once training is identified.

Resource Estimate ($ in Millions):

Type	FY11	FY12	FY13	FY14	FY15	FY16
Civilian Overtime	0	1.2	1.2	1.2	1.2	1.2
Training Support Package Contractor Support	0	.175	.175	.175	.175	.175
Total	0	1.375	1.375	1.375	1.375	1.375

6) **Finding 3.8.A - The DoD does not have a policy governing privately owned weapons.**

Recommendation 3.8.A - (OTJAG and ACSIM in support) Review the need for a DoD Privately Owned Weapons policy.

Discussion: DoD has established draft policy on the carrying and registration of privately owned weapons on DoD installations. OPMG has reviewed this policy and will recommend Secretary of the Army concur with comments: "Installation Commanders have clear authority and responsibility to regulate privately owned weapons on installations. DoD policy should direct that privately owned weapons registration is mandatory for personnel who reside on the installation as well as those who have a need (hunting, use of ranges or other legal purposes) to bring weapons onto the installation."

The Army and other Services have previously established privately owned weapons policies which set minimum standards that regulate privately owned weapons, explosives, or ammunition on individual installations.

The Army has policy (AR 190-11, "*Physical Security of Arms, Ammunition, and Explosives*") that prohibits the carrying of privately owned weapons, explosives, or ammunition on military installations unless authorized by the installation commander. The Army policy requires posted notices to be at installation access control points reinforcing this prohibition. The Army requires Commanders to establish procedures that regulate privately owned weapons, explosives, or ammunition on the installation and mandate the registration of firearms belonging to personnel living on the installation, to include procedures for hunters and others using installation firing ranges. The Army also requires commanders to post applicable local laws and regulations on the ownership, registration and possession of weapons and ammunition on unit bulletin boards.

Army policy does not require Army personnel who reside off-post to register privately owned weapons or ammunition. These personnel are required to comply with federal, state and local laws concerning ownership, possession, registration, off-post transport and use. ACOMs have also voiced legal (2nd Amendment conflict) and practical (enforceability) reasons why privately owned weapons registration should not be directed for Army personnel who reside off-post. However, installation commanders have clear authority and responsibility to regulate privately owned weapons on installations. OPMG will revise policy to direct that privately owned weapons registration is mandatory for personnel who reside on the installation as well as those who have a need (hunting, use of ranges or other legal purposes) to bring weapons onto the installation. The anticipated review will be completed by 30 August 2010 and the revision to AR 190-11 is anticipated to be published by 30 November 2010.

Key action necessary to implement the recommendation includes:

- (D) OPMG is staffing a revision to current policy (AR 190-11) that would require the registration of privately owned weapons by personnel who reside on an Army installation as well as who have a need (hunting, use of ranges or other legal purposes) to bring weapons onto the installation.

7) **Finding 3.9 - Services cannot share information on personnel and vehicles registered on installation, installation debarment lists and other relevant information required to screen personnel and vehicles and grant access.**

Recommendation 3.9.A - (G-1, G-2 and ACSIM in support) Develop timely information sharing capabilities among components including vehicle registration, installation debarment lists

and other access control information. **(Note: This recommendation requires OSD action before the Army can implement)**

Recommendation 3.9.B - (G-1, G-2 and ACSIM in support) Accelerate efforts to automate access control that will authenticate various identification media (e.g., passports, Common Access Card, drivers' licenses, license plates) against authoritative databases.

Recommendation 3.9.C. - (G-2 in support) Obtain sufficient access to appropriate threat databases and disseminate information to local commanders to enable screening at continental United States and overseas installation access control points.

Discussion: OPMG is working with the DoD Physical Security Equipment Action Group's Defense Installation Access Control Working Group to define a cross-service interoperable access control enterprise architecture. The goal is to field interoperable installation physical access control systems that can access the Defense Manpower Data Center's Defense Enrollment Eligibility Reporting System to facilitate Common Access Card validation. The Defense Installation Access Control Working Group will be meeting during May-November 2010 to define among the Services the end-state concept for access control enterprise architecture for joint interoperability. This effort is expected to generate required changes for DoD Access Control Policy, define requirements to build debarment and local population databases and identify equipment and technology. The end state will be a recommended solution (middleware/enterprise/standard interface) for physical access control systems to use that can share access control information with the other Services.

OPMG is fielding automation to authenticate identification cards against DoD databases, thus improving security as well as reducing guard requirements. This system is called Automated Installation Entry and will improve vehicle throughput, reduce manpower requirements and comply with DoD guidance and Congressional direction. This system was first fielded at Fort Hood. There are Product Verification Tests ongoing at Letterkenny Army Depot, Fort Campbell and the Military Ocean Terminal at Sunny Point. Fielding is expected in FY 2010 - 2011. The OPMG developed Automated Installation Entry requirements for 18 additional installations for POM 12-16. In addition, OPMG will submit requirements for handheld screening systems at the remaining CONUS installations once a viable multiservice concept and interoperable middleware are developed.

Army OPMG is implementing DoD policy and working several efforts simultaneously to gain access to threat screening databases for access control.

OPMG is publishing an update of Chapter 8 (Access Control) to AR 190-13, "*Physical Security*," that will implement the DoD Directive Type Memorandum requirement to screen non-Common Access Card holders. Installations are required to query authoritative government data bases (NCIC) which includes a check against the terrorist screening database in order to vet a non-Common Access Card cardholder's claimed identity and determine their fitness for access. The FBI permits the use of NCIC for vetting visitors to ensure the security of military installations. The Army will publish the revised AR 190-13 no later than 30 August 2010.

The Army OPMG is participating in the USD(I) led effort to field the Justice Communications Systems. Justice Communications Systems is a store and forward information sharing system which interfaces with the Federal Bureau of Investigation CJIS NCIC and the International Justice and Public Safety Network as well as the National Law Enforcement Telecommunications System. This will enable a rapid method for verifying a person's crimi-

nal and personnel records status for access control. Justice Communications Systems is web based and allows the transmittal of batch files of names for screening against NCIC records. A pilot program of Justice Communications Systems began in May 2010 at Fort Campbell and in USAREUR at Campbell Barracks. Justice Communications Systems currently charges a fee per name check which is expensive, but once it is fully implemented costs should be reduced. Department of Justice's Justice Communications Systems capability could potentially provide accounts and vetting capability for all Army installation visitor control centers. USD(I) will finalize an MOU with Department of Justice in August 2010 and plans to enable fielding at all installations across DoD in FY 2011.

OPMG is working with CID, United States Forces-Korea, USAREUR and the FBI to provide NCIC access to overseas locations which until now have not had such access. This effort will field hardware, software, licensing, training and system accreditation in support of the United States Forces Korea PM's Office no later than 30 September 2010. This is the first step of a multi-phased plan to provide NCIC access to locations in Korea and in Europe.

Additionally, on 27 January 2010 the Provost Marshal General requested USD(I) assistance in helping Army overseas commands gain direct access to the Terrorist Screening Center's terrorist screening database. USAREUR, United States Eighth Army in Korea and United States Army Central require this capability to screen personnel desiring access to Army bases that do not have a Common Access Card. The plan calls for DoD guards (to include foreign contract guards) to use the terrorist screening database to screen personnel entering our installations. USD(I) is developing business rule requirements to store, update and safe guard information which will be governed in accordance with a MOU with the Department of Justice/ Terrorist Screening Center.

Key actions necessary to implement the recommendation include:

- (D) Maneuver Support Center of Excellence will update FM 3-19.30, "*Physical Security*," to reflect the changes to AR 190-13.
- (D) OPMG Revised AR 190-13, "*The Army Physical Security Program*," to incorporate access control identification vetting and proofing requirements in accordance with USD(I) Directive-Type Memorandum 09-012, "*Interim Policy Guidance for DoD Physical Access Control*." AR 190-13 is currently at the Army Publication Directorate, but any new policy coming out of the Defense Industry Access Control Working Group events would require another rapid revision. OPMG also issued a message that implements Directive Type Memorandum 09-012 (ALARACT message 049 2010 "*Guidance for Physical Access Control for Army Installations,*" 191713Z FEB 10).
- (T) Training for Automated Installation Entry occurs during implementation at installations. Training costs are included in the total cost of Automated Installation Entry fielding.
- (T) United States Army Crime Records Center will oversee local training plans for military police personnel who will have access to NCIC.
- (M) The adoption of a recommended solution (middleware/enterprise/standard interface) for service personnel access control systems to use that can share access control information with other Services may require adjustments to existing and future access control automation specifications. OPMG will work with Product Manager, FP Systems and the United States Army Corps of Engineers to incorporate changes.

The Defense Installation Access Control Working Group met 17-19 May 2010 and is cur-

rently finalizing best practices and has followed with a capability demonstration in June 2010. Services will now be able to select the best option for physical access control architecture and methods for sharing access control information. OPMG anticipates that as commanders and security forces employ automation for access control they will find innovative ways to improve efficiency/traffic throughput and further reduce guard forces. OPMG will review best practices, and if adopted, will make policy updates. OPMG will determine best practices implementation and review of Phase I NCIC access in United States Forces Korea after the 30 September 2010 implementation date.

The Defense Installation Access Control working group and Physical Security Equipment Action Group are developing resource requirements as the architecture develops. OPMG is conducting a cost-benefit analysis to define options for program costs for the II PEG.

Installations will submit requirements in November and December of 2010 to field NCIC databases at visitor control centers. However, the fielding of the Justice Communication System could potentially reduce costs since existing internet capability is the only materiel requirement. Overseas installations are developing funding requirements for the NCIC program. Phase I implementation is projected to cost $350,000. OPMG will program future costs during the Program Objective Memorandum cycle in FY 2011 through the II PEG, Physical Security MDEP.

Recommendation Milestones:

3.9.A - The Defense Installation Access Control Working Group will meet during May-November 2010 to define the concept for access control enterprise architecture for joint interoperability. This working group will also conduct a series of demonstrations from June-November 2010 that will assess options for a Physical Access Control Architecture that specifically includes the ability to exchange data between Service Personnel Access Control Systems and an authoritative source. The end state of the Defense Installation Access Control demonstrations should be a recommended solution (middleware/enterprise/standard interface) for Service Personnel Access Control Systems to use that can share access control information with the other Services. Based on the results of the Defense Installation Access Control working group demonstrations in 2010, DoD will likely publish changes to policy and system standards that the Services may have to follow in fielding future access control systems.

OPMG in coordination with G-3/5/7 and IMCOM will develop a strategy to communicate to installation commanders the cross-service interoperable access control enterprise architecture requirements that will affect their installations.

3.9.B - United States Army Corps of Engineers is installing Automated Installation Entry at Fort Campbell and Military Ocean Terminal at Sunny Point during FY 2010.

Program Manager for FP Systems will begin to field Automated Installation Entry at ten additional installations during FY 2010.

OPMG submitted requirements for fielding Automated Installation Entry at 18 installations during FY 12-16 through the Installation PEG.

OPMG and the United States Army Corps of Engineers will develop a strategy to communicate to installation commanders the Automated Installation Entry schedules and engineer site preparation requirements that will affect their installations prior to Automated Installation Entry fielding.

The United States Army Corps of Engineers and OPMG will develop and approve specifications and performance metrics for Automated Installation Access.

3.9.C - Policy Guidance: OPMG published an ALARACT message on Access Control to implement guidance in accordance with DoD Directive Type Memorandum on Access Control released in January 2010. The Army OPMG will revise AR 190-13, "Physical Security," Chapter 8 (Access Control) by 30 August 2010.

Overseas National Criminal Information Center Fielding: Approval of Phase I funding – April 2010 (completed), completion of phase I NCIC access to United States Forces-Korea PM Office: 30 September 2010 (ongoing), phases II-IV to be determined after second quarter FY 2011 assessment of administrative workload based on Phase I usage.

Justice Communication Systems: Pilot Programs at Fort Campbell, Kentucky and USAREUR (May - October 2010); fielding at installations across the Army in FY 2011.

Resource Estimate: OPMG submitted requirements for fielding Automated Installation Entry at 18 installations in Program Objective Memorandum 12-16. Requirements for threat assessment database fielding are being developed as implementation of overseas installation NCIC program occurs. Phase I implementation is projected to cost $350,000.

8) **Finding 4.3 - DoD policy does not currently take advantage of successful models for ASR for civilian and military law enforcement on DoD installations and facilities.**

Recommendation 4.3.A - Identify and incorporate civilian law enforcement best practices, including ASR, into training certifications for civilian police and guards.

Recommendation 4.3.B - DoD policy does not currently take advantage of successful models for ASR for civilian and military law enforcement on DoD installations and facilities.

Recommendation 4.3.C - Incorporate the Department of Homeland Security best practices regarding workplace violence and active shooter awareness training into existing personal security awareness training contained in current Level 1 Antiterrorism Awareness training.

Recommendation 4.3.D - Case study will be developed to provide DoD with a guide for installation commander development and on-scene commander response program.

Discussion: The Army conducted extensive research and incorporated federal, state and local law enforcement best practices into the training curriculum, including ASR, for Army civilian police, security guards and MPs.

After the 9/11 attacks, the Army created the United States Army Civilian Police Academy in order to provide professionally trained and physically fit law enforcement and security personnel to serve as first responders to acts of terrorism and crime directed against Army installations/activities. The mission of the academy is twofold: 1) to conduct law enforcement and security skills training, using proven best practices developed by civilian and military law enforcement agencies; and 2) to enable Department of the Army and DoD agencies to perform their law enforcement, physical security, antiterrorism and FP missions.

The USAMPS developed an ASR TSP in March 2010 and instructs DACPs during the 9-week certification course. The USAMPS also released the Field Training Program in order to train the DACP previously certified and for MPs in the field. The TSP is a 14-hour training package, developed by USAMPS using best practices adopted from diverse law enforcement agencies such as the United States Secret Service, the FBI and the El Paso County Sheriff's

Department. The TSP provides commanders, PMs and Directors of Emergency Services a model for training their military and civilian police to respond to the threat of an active shooter or other incidents involving workplace violence. Several recent events and, especially the attack at Fort Hood, validated the need for this proactive training measure to protect the Soldiers, Civilians and Family members who serve and live on Army installations. Using an analysis of active shooter events going back to the 1980s and capturing modern industry best practices for standard tactics, techniques and procedures, USAMPS takes a multi-disciplined approach to training first and second tier responders.

An OPMG memorandum, dated 30 March 2010, mandated this training for DACPs, security guards and MPs performing law enforcement and security duties on installations world-wide. OPMG Policy Division seeks to rapidly revise AR 190-56, "*The Army Civilian Police and Security Guard Program,*" to include the active shooter training requirement and expects to staff the draft revision in the fourth quarter FY 2010 with anticipated publication by 31 December 2010. OPMG Policy will also seek to revise AR 190-14, "*Carrying of Firearms and Use of Force for Law Enforcement and Security Duties*," by 31 December 10 to address ASR and other acts of interpersonal violence for all Army military and civilian law enforcement and security personnel. USAMPS has incorporated training for military law enforcement personnel in July 2010.

The Army has also incorporated best practices regarding active shooter awareness and workplace violence training into existing personal security awareness training contained in Level I Antiterrorism Awareness training.

USAMPS completed a case study of the Fort Hood shooting incident. This case study represents a review of on-scene command actions and objectives based upon the active shooter incident which occurred at Fort Hood, Texas on 5 November 2009. It examines emergency first responder on-scene command actions and applies the NIMS and the Incident Command System protocols to the Fort Hood active shooter scenario. While the incident could have occurred on any installation, at any time, the Fort Hood scenario is utilized only as a point of reference to indicate how the NIMS and the Incident Command System influences and informs the concept of incident and/or on- scene command during an emergency.

Key actions necessary to implement the recommendation include:

- (D) Maneuver Support Center of Excellence will revise FM 3.19-39, "*Army Law and Order,*" with an estimated publication in second quarter, FY 2011.
- (D) Updated training standards are contained in the soon to be published Multi Service Regulation, AR 190-60, "*Minimum Training, Certification, and Physical Fitness Standards for Civilian Police and Security Guards in the DoD*."
- (D) OPMG will revise AR 190-56, "*Army Civilian Police & Security Guard Program*," for training requirements and AR 190-14, "*Carrying of Firearms & Use of Force for Law Enforcement & Security Duties,*" for response to active shooter/other emergency, life threatening situations in first quarter FY 2011.
- (D) OPMG will publish a multi-service regulation AR 190-60, "*Minimum Training, Certification and Physical Fitness Standards for Civilian Police & Security Guards in the DoD,*" in response to the DoD Instruction 5210.90.
- (O) Develop the charter for and form the DoD Law Enforcement Training Advisory Council.

Resource Estimate: The ASR TSP will require funding estimated at $2.1 million in overtime pay. Additional resources include programming for training ammunitions (blanks/simunitions with barrels to support training).

F. OTSG Lead:

1) **Finding 2.13 - Commanders and military healthcare providers do not have visibility on risk indicators of Service members who seek care from civilian medical entities.**

Recommendation 2.13.A - Consider seeking adoption of policies and procedures to ensure thorough and timely dissemination of relevant Service member violence risk indicators from civilian entities to command and military medical personnel.

Discussion: In March 2009, the Army's OTSG issued Policy Memorandum 10-024, "*Case Management for soldiers referred to the network for behavioral health care*." This policy defines how behavioral health information is shared and requires the Soldier to authorize access to medical information as a condition of treatment outside of the military treatment facility.

As outlined in Appendix D, Manpower & Reserve Affairs discussion of finding and recommendation 2.1.A, the Army will also issue interim guidance to commanders and supervisors on behavioral indicators of violence.

Civilian health care entities may release healthcare information about a Soldier to military command authorities "for activities deemed necessary by appropriate military command authorities' proper execution of the military mission," or for duty or mission performance. DoD regulation 6025.18-R, Chapter C7 sets forth the criteria for release of information.

Key action necessary to implement the recommendation includes:

- (D) Address identification of violent behavior indicators, contributing factors, or prevention of workplace violence by March 2011. (Lead: ASA(M&RA))

2) **Finding 5.1.A - DoD installations are not consistent in adequately planning for mental health support for domestic mass casualty incidents to meet needs of victims and families.**

Recommendation 5.1.A - (G-3/5/7 in support) Update mental health care clinical practice guidelines that address both combat and domestic incidents to ensure current and consistent preventive care.

3) **Finding 5.1.B. - At Fort Hood, advanced treatment protocols developed at our universities and centers were not available to the commander prior to the incident.**

Recommendation 5.1.B. - (G-3/5/7 in support) Review best practices inside and outside DoD to develop policies, programs, processes and procedures to provide commanders tools required to protect the force in the aftermath of combat or mass casualty incidents.

4) **Finding 5.1.C. - Fort Hood developed a behavioral health plan that incorporated current practices including a "whole of community" approach, and a strategy for long-term behavioral healthcare not reflected in any DoD policy.**

Recommendation 5.1.C. - (G-3/5/7 in support) Consider Air Force Instruction and the Fort Hood Behavioral Health Campaign Plan as possible sources for developing appropriate guidance.

Discussion: In May 2010, the Army's Medical Department Center and School conducted

the first 40 hour TEM Course for behavioral health providers and Unit Ministry Teams in response to requirements identified in AR 525-27, "*Army Emergency Management Program*," 13 March 2009. As of 18 June 2010, the Army Medical Center and School has conducted this resident course twice. The resident course is scheduled to be conducted ten times per year with two military training teams for non-resident training. MEDCOM will monitor completion through the Digital Training Management System. Regional Medical Commands will report course completion semi-annually to the OTSG Behavioral Health Proponency for analysis and improvement.

OTSG is developing the Comprehensive Behavior Health System of Care Campaign Plan that will more clearly delineate existing policies, procedures and guidance to establish minimum standards for TEM. Following the Independent Review Panel's report, OTSG incorporated recommendation 5.1.C. into the plan.

Additionally, OTSG/MEDCOM policy "Combat Operational Stress Control Training for Behavioral Health Personnel," 29 December 2008, in response to the Suicide Task Force Task 1.27.2, requires pre-deployment training for all behavior health personnel. Based on FM 4-02.51, "*Combat Operational Stress Control*," July 2006, Combat Operational Stress Control Training is composed of any one of three courses that enable behavioral health personnel to better manage stress in a deployed environment.

Key actions necessary to implement the recommendation include:

- (D) The Army Campaign Plan integrates the Comprehensive Behavior Health System of Care Campaign Plan. (Lead: OTSG)
- (D) Headquarters Department of the Army issues an Execution Order to implement the Behavioral Health System of Care Campaign Plan. OTSG Behavioral Health Proponency will monitor the plan for quality assurance.
- (D,T) Upon completion of review, the AMEDD Center and School will publish the MEDCOM's TEM manual. OTSG must approve the manual. (Lead: MEDCOM)

5) **Finding 5.2.A - DoD does not have comprehensive policies that recognize, define, integrate and synchronize monitoring and intervention efforts to assess and build healthcare provider readiness.**

Recommendation 5.2.A - Create a body of policies that: recognizes, defines and synchronizes efforts to support and measure healthcare provider readiness in garrison and deployed settings.

6) **Finding 5.2.B - DoD does not have readiness sustainment models, with requisite resources, for the health provider force that are similar to readiness sustainment models for combat and combat support forces.**

Recommendation 5.2.B - Address individual assessment, fatigue prevention, non-retribution, reduced stigma for those seeking care and appropriate procedures for supporting clinical practice during healthcare provider recovery.

7) **Finding 5.2.C - The demand for support from caregivers in general, and from mental healthcare providers in particular is increasing and appears likely to continue to increase due to the stress on the military personnel and their families from our high operational tempo and repeated assignments to combat areas.**

Recommendation 5.2.C - Required DoD and Uniformed Services University of Health Sciences curricula, training materials and personnel performance management systems to incorporate healthcare provider self-care skills and readiness concepts.

8) **Finding 5.2.D - The demand for support from caregivers in general, and from mental healthcare providers in particular is increasing and appears likely to continue to increase due to the stress on the military personnel and their families from our high operational tempo and repeated assignments to combat areas.**

Recommendation 5.2.D - Develop mechanisms for collaborating with civilian resiliency resources.

Discussion: OTSG and MEDCOM reviewed recommendations 5.2.A and 5.2.B. and determined that the existing DoD and ARs, instructions and manuals are appropriate. MEDCOM considers the TEM Course, as described in the discussion for recommendation 5.1C, to be responsive and appropriate for recommendations 5.2.B - D.

OTSG and MEDCOM find that Care Provider Support training responds appropriately to 5.2.C. Care Provider Support training, established by MEDCOM fragmentary order 34 to operation order 07-55, 27 June 2008, is an annual requirement for all healthcare providers and teaches healthcare providers how to manage the unique stressors associated with providing health care. MEDCOM monitors completion through the Digital Training Management System. Regional Medical Commands will report course completion semi-annually to the OTSG Behavioral Health Proponency for analysis and improvement.

Programs responsive to recommendations 5.2.C. and 5.2.D. are available to all Soldiers including Army healthcare providers. These programs include: the CSF program, adopted Army-wide in October 2009; the Military One Source telephone information center and website and the voluntary online behavioral health website: MilitaryMentalHealth.org; and self-referral to the assistance provided by Military and Life Consultants through ACS.

9) **Finding 5.3 - The lack of a readiness sustainment model for the health provider force, the unique stressors that healthcare providers experience, and the increasing demand for support combine to undermine force readiness- care for both warriors and healthcare providers.**

Recommendation 5.3.A - Develop integrated policies, processes and properly resourced programs to sustain high quality care.

Recommendation 5.3.B - (G-1 in support) Develop a deployment model that provides recovery and sustainment for healthcare providers comparable to that provided to the combat and combat support components of the force.

Recommendation 5.3.C - Review the requirement for DoD to destigmatize healthcare providers who seek treatment for stress.

Discussion: OTSG and MEDCOM reviewed recommendations 5.3.A - C and determined that the components of the Comprehensive Behavior Health System of Care Campaign Plan appropriately address the concerns within these recommendations. Campaign Plan components already implemented include, but are not limited to: 1) the TEM Course, established in May 2010; 2) the Care Provider Support Training, established in June 2008; 3) the Combat Operational Stress Course; 4) the CSF program, adopted Army-wide in October 2009; and 5) all Soldier programs relevant to behavioral health self-referral.

10) **Finding 5.4 - Senior caregivers are not consistently functioning as clinical peer and mentors to junior caregivers.**

Recommendation 5.4.A - Review Senior Medical Corps officer requirements to determine optimal roles, utilization and assignments.

Discussion: OTSG and MEDCOM reviewed this finding and recommendation and found that

75% of its senior Medical Corps officers defined as those in the rank of lieutenant colonel promotable or colonel are working in clinical positions and functioning as clinical peers and mentors to junior caregivers. Additionally, DA PAM 600-4, "*AMEDD Officer Development and Career Management*," set an appropriate standard for senior Medical Corps officer assignments.

G. ACSIM Lead:

1) Finding 4.8 - DoD has not produced guidance to develop family assistance plans for mass casualty and crisis response. As a result, Service-level planning lacks consistency and specificity, which leads to variation in the delivery of victim and family care.

Recommendation 4.8.A - (G-3/5/7 in support) Develop guidance incorporating the core service elements of a FAC as identified in the Pentagon AAR.

Discussion: The Army FACs are not a new requirement in ACS Centers. AR 608-1 requires FACs, ACS Centers, FAC standard operating procedures, FAC planning, ACS Accreditation Standards and an Installation Emergency Plan. However, the Army has not incorporated all the functional areas identified in the 9/11 Pentagon FAC after action report.

The Pentagon FAC after action review identified a requirement for synchronizing and coordinating the following 13 functional areas: administration, Casualty and mortuary assistance, child care, C2, communications and IT, community outreach (e.g. medical, mental health, chaplain), donations management, legal assistance, logistics and operational support, public affairs, resource management, security, staff and volunteer management.

Most of the installation's FACs that the team visited had published SOPs in the event of a crisis or mass casualty events; however, some were in the process of being updated. Flexibility is the key in adapting to different situations. Most installations' SOPs addressed the provision of minimum services to Family members to include emergency financial assistance, crisis referral, legal services, ID Cards, medical TRI-Care assistance, ACS program services and other community resources. However, we learned that the majority of the installations visited are primarily focused on providing support to post-wide mobilizations and are able to quickly transition services to respond to any crisis situations. FACs are included in installation-wide training exercises to include mass casualty exercises.

In anticipation of the DoD guidance to update FACs, which is scheduled to be published in December 2010, the Army is updating AR 608-1, "Army Community Service Centers" to read the following:

"FACs provide a coordinated humanitarian response to major events in the military community. They are one-stop sites where Soldiers and Families can receive accurate information in a sensitive, timely and effective manner. FACs provide concrete logistical and emotional support. Planning for family assistance will ensure a comprehensive, effective and coordinated delivery system. Typical services provided at the FAC are information and referral; legal; pastoral; child, youth and school services support; housing; transportation; behavioral health; financial and casualty support." Family assistance plans should include:

- Demonstration of ability to adapt to different types of emergencies, such as mass casualties, evacuations, natural disasters and acts of terror.
- Resource requirements for personnel, equipment, IT support, communication and facilities.
- Contingency plans for both on and off post FACs. Sites will have adequate phone lines,

meeting rooms, private counseling space, child care areas and refreshment space.

- Activation procedures, with clear C2 guidelines.
- Communications plans, both to command and other emergency response agencies.
- Plans to communicate with impacted Families.
- Standards for screening and training FAC staff, to include volunteers.
- Donation management procedures.
- Public Affairs coordinating procedures.
- Data and reporting requirements, which includes a client tracking system.
- Security operations procedures.
- Coordination with key Civilian, Military, federal, state and local agencies, to include the Reserve Components.
- FAC closure and transition to long-term needs support procedures.

FAC plans will be included in the installation emergency planning procedures. Additionally, the FAC plan will be tested in installation emergency preparedness exercises annually.

Recommended changes to AR 608-1, Chapter 4, paragraph 4-1, 4.2 and 4-4. Additionally, AR 608-1, Appendix F will be revised with further operational guidance.

The USD(P&R) will revise of DoDI 1342.22 "*Family Centers*" by December 2010. ACSIM will review and update AR 608-1 IAW DoD guidance.

Key actions necessary to implement the recommendation include:

- (D) Complete recommended changes to AR 608-1, Chapter 4, paragraph 4-1, 4.2 and 4-4. Additionally, AR 608-1, Appendix F will be revised for further operational guidance.
- (O) The ACS FAC Annex is included in the overall Installation Emergency Plan. The installation commander has the authority to establish a FAC. The FAC Plan establishes organization roles and responsibilities, resource requirements and communication capabilities/requirements. The FAC SOP establishes operational guidance.
- (T) ACS center directors have training plans established to exercise their FAC Plan and validate their FAC SOP annually.
- (M) The FAC Plan will use existing equipment.
- (T) Annual exercise supplemented by installation/community testing of installation and community emergency plan.
- (P) FAC Plan indicates the required number of staff. Staffing requirements are based on operating hours and mission/type of operation.
- (F) Installations have pre-determined on and off post locations. On-post is required, off-post is recommended.

2) Finding 4.8 - DoD has not produced guidance to develop family assistance plans for mass casualty and cri-

sis response. As a result, Service-level planning lacks consistency and specificity, which leads to variation in the delivery of victim and family care.

Recommendation 4.8.B - (G-3/5/7 in support) Develop guidance to establish a FAC response as a component to the IEM program.

Discussion: There is no information in AR 525-27, "*Army Emergency Management*," that provides guidance on establishing FACs during a crisis or threat situation. Listed below is the recommended FAC guidance information that must be included in AR 525-27 on page 4, paragraph 1-18 Installation Commanders, add sections n-u "Installation Commanders will:"

- Ensure FACs provide a coordinated response to major events in the military community. FACs are one-stop sites where Soldiers and Families receive accurate information in a sensitive, timely and effective manner.
- Ensure that FACs are part of the annual Installation Emergency Planning Exercises.
- Ensure clear FAC activation procedures and guidelines are established and communicated to installation staff, Family members and Soldiers.
- Ensure FACs have resources to provide logistical and emotional support in the event of mass casualties, natural disasters, acts of terrorism and evacuations. Resource requirements include: personnel, equipment, IT support, communication, security and facilities (both on and off the installation)
- Ensure that the FAC provides, at a minimum, these services: information and referral, legal, pastoral, child care assistance/referral, housing, transportation, behavioral health, financial and casualty support.
- Ensure that donation management procedures are established.
- Ensure coordination with key civilian and military agencies, as well as Reserve Component counterparts, for emergency planning, crisis response and after action review.
- Ensure that Child, Youth and School Services are part of the Mobilization and Contingency Plan."
- Update AR 525-27, Appendix A, page 15, add: AR 608-1, Army Community Service Centers
- Update AR 525-27, Glossary Section 1, Abbreviations, page 17.dd: FAC: Family Assistance Center.
- Update AR 525-27, Glossary Section II, Terms, page 22, add: Family Assistance Centers: FACs provide a coordinated response to major events in the military community. They are one-stop sites where Soldiers and Families can receive accurate information in a sensitive, timely and effective manner. FACs provide concrete logistical and emotional support. Planning for Family assistance will ensure a comprehensive, effective and coordinated delivery system. Typical services provided at the FAC are information and referral, legal, pastoral, child, youth and school services support, housing, transportation, behavioral health, financial and casualty support.

  The Under Secretary of Defense (Acquisition, Technology, and Logistics) has initiated formal coordination on updates to DoDI 6055.17, "DoD Installation Emergency Management Program," to ensure FAC crisis and mass casualty response plans become integral elements of the IEM program and will provide guidance to all the Services by December

2010. ACSIM will update its regulations in accordance with DoD guidance.

Key actions necessary to implement the recommendation include:

- (D) Review AR 525-27 and add FAC operations for EM guidance.
- (O) The ACS FAC Annex is included in the overall Installation Emergency Plan. The installation commander has the authority to establish a FAC. The FAC plan establishes organization roles and responsibilities, resource requirements and communication capabilities/requirements. The FAC SOP establishes operational guidance.
- (T) ACS center directors have training plans established to annually exercise their FAC plan and validate their FAC SOP.
- (M) The FAC Plan will use existing equipment.
- (L) Supplement the annual exercise with installation/community testing of installation and community emergency plan.
- (P) FAC Plan indicates the required number of staff. Staffing requirements are based on operating hours and mission/type of operation.
- (F) Installations have pre-determined on and off post locations. On-post is required, off post is recommended.

3) **Finding 4.8 - DoD has not produced guidance to develop family assistance plans for mass casualty and crisis response. As a result, Service-level planning lacks consistency and specificity, which leads to variation in the delivery of victim and family care.**

Recommendation 4.8.C - (G-3/5/7 in support) Consider USAF emergency FAC and Fort Hood as best practices.

Discussion: The DoD directed that the FAC crisis and mass casualty response "establish procedures to integrate victim and family services in response to the full spectrum of crisis or catastrophic events." The USD(P&R) will review and identify Service best practices and revise DoDI 1342.22, "*Family Readiness Program*," to incorporate best practices model for a FAC by December 2010.

ACSIM assessed FAC operations across its installations and recommends the following Army best practices as inclusion to DoD identified best practices for FAC Operations or elements of a FAC:

- Fort Myer, Fort Richardson and Schofield Barracks have some of the best examples of Family Assistance Plans, as they provide clear operational guidelines for a FAC.
- Fort Bliss has nine teams consisting of 6-7 members each comprising a cross-section of ACS members. The teams receive monthly FAC operational training. This was observed at the Fort Bliss installation visit by the Fort Hood Task Force.
- Specific sections of the Joint FAC plan, Navy Plan, Air Force Plan and Fort Drum plan contain aspects that should be considered for inclusion in FAC plans.
- The Navy clearly delineated the chain of command.
- The Air Force and Joint FAC Models have checklists for review.

- The Fort Drum plan has detailed appendices in the Family Assistance Plan.
- The Joint FAC has an organization chart which is beneficial.
- The NORTHCOM Plan provides an example of the "big picture" for the Army.
- Recommend adopting the Army Disaster Personnel Accountability & Assessment System for client tracking.

The Army submitted its best practice recommendations to the DoD for implementation at all DoD FAC. We recommend the USD(P&R) review and identify Service best practices and revise DoDI 1342.22, "Family Readiness Program," to incorporate best practices model for a FAC by December 2010.

Key actions necessary to implement the recommendation include:

- (D) Recommended best practices to be included in the DoD-wide published best practices for improving FAC operations during a crisis.
- (O) The ACS FAC Annex is included in the overall installation emergency plan. The installation commander has the authority to establish a FAC. The FAC plan establishes organization roles and responsibilities, resource requirements and communication capabilities/requirements. The FAC SOP establishes operational guidance.
- (T) ACS center directors have training plans established to annually exercise their FAC plan and validate their FAC SOP.
- (M) The FAC plan will use existing equipment.
- (L) Supplement the annual exercise with the installation/community testing of installation and community emergency plan.
- (P) FAC Plan indicates the required number of staff. Staffing requirements are based on operating hours and mission/type of operation.
- (F) Installations have pre-determined on and off post locations. On-post is required, off-post is recommended.

Appendix E (Army Directive 2008-02 Army Protection, 9 April 2008) to Fort Hood Army Internal Review Team Report)

SECRETARY OF THE ARMY
WASHINGTON

09 APR 2008

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2008-02 – Army Protection

1. The goal of this directive is to synchronize all Army protection-related functions into a coherent program to maximize the security of Soldiers, civilians, their Families, infrastructure and information from all hazards, including traditional, irregular, disruptive and/or catastrophic attacks. In order to coordinate and synchronize all Army protection functions, the Army will incorporate the protection goals and objectives into Headquarters, Department of the Army protection policy and processes.

2. In the 2006 National Security Strategy, the President noted that many of the threats we face today, such as weapons of mass destruction, terrorism, pandemic disease, and natural disasters, reach across borders. Our response to these threats must reach across traditional boundaries within the Army. Our protection goals and objectives will enable the Army to better protect personnel, infrastructure, and information from all hazards, so we can effectively respond when required and accomplish our mission.

3. As part of the Army's transformation and to enhance our effectiveness in the Global War on Terrorism, we must better coordinate and synchronize all Army protection efforts at all levels.

4. The DCS, G-3/5/7 is the staff agent for Army Protection Policy.

Pete Geren

Encl
Army Protection Policy Guidance

DISTRIBUTION:
HQDA Principal Officials
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Europe
(CONT)

Appendix E

SUBJECT: Army Directive 2008-02 – Army Protection

DISTRIBUTION: (CONT)
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Pacific
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
Eighth U.S. Army
U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
U.S. Army Medical Command/The Surgeon General
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Reserve Command
U.S. Army Installation Management Command
Superintendent, U.S. Military Academy
Director, U.S. Army Acquisition Support Center

Appendix E

Army Protection Policy Guidance

1. Background.

a. In 2006, the Director of the Army Staff (DAS) directed a Protection Integrated Process Team (IPT) be formed to establish a plan for holistic force protection. The Protection IPT developed six Protection goals and sixteen objectives to synchronize Army Protection efforts. (See Annex, Protection Goals and Objectives)

b. In 2007, the G-3/5/7 approved and endorsed the Army Strategy for Protection.

c. In January 2008, the Chief of Staff of the Army endorsed the Protection Strategy and recommended that the Protection goals and objectives be incorporated into an Army Directive. This Directive is predicated upon the following key assumptions:

(1) Traditional aggressors, terrorists, criminals and natural disasters will continue to pose a threat to our Soldiers, civilians, their Families, infrastructure, and information.

(2) The Army must better utilize competing resources.

2. References.

a. US Army Audit Agency Report: A-2007-0177-FFD, Roles and Responsibilities for Force Protection, 30 July 2007.

b. Army Protection White Paper, 25 January 2008.

3. Policy.

It is Department of the Army policy to develop and employ all measures to prevent an attack and minimize the risks from all hazards to our Soldiers, civilians, their Families, infrastructure, and information, to achieve mission assurance. In order to better adapt to an evolving threat environment and to achieve a broad, coherent, and comprehensive approach to protection, the Army adopts an all hazards approach to protection. An all hazards approach to protection focuses on protecting personnel, infrastructure and information from traditional, irregular, disruptive, and catastrophic threats, to include criminal activity and naturally occurring disasters. The Army will prepare to recover quickly should prevention and protection efforts fail.

4. Procedures.

The ARSTAF, led by the G-3/5/7, will develop procedures for meeting the Army Protection Goals and Objectives. Once the ARSTAF has established its synchronized Protection processes and procedures, an Army Regulation on Protection will be developed and released to clearly identify roles, responsibilities and relationships across the Headquarters, Department of the Army (HQDA) staff.

Appendix E

Army Protection Policy Guidance

5. Responsibilities.

The G-3/5/7 is the Army proponent for Protection policy, priorities, and resources. The G-3/5/7 will coordinate with the Army Staff (ARSTAF) in order to establish the elements of Protection at the HQDA level.

a. The G-3/5/7, Army Asymmetric Warfare Office (AAWO), Force Protection Division, will coordinate and synchronize Army-wide Protection efforts. The AAWO is the lead office for accomplishing Goals 1, 2, 3, 5, and 6, and will assist the G-8 with Goal 4.

b. The G-1 will provide administrative support to other staff members assigned to lead or assist on Protection tasks.

c. The G-2 will assist the G-3/5/7 and G- 8 with Goals 1, 3, 4, and 5.

d. The G-4 will assist the G-3/5/7 and G-8 with Goals 1, 4 and 5.

e. The CIO/G-6 will assist the G-3/5/7 with Goals 1, 5 and 6.

f. The G-8 will lead the accomplishment of Goal 4.

g. The Assistant Secretary of the Army (Financial Management and Comptroller) / Army Budget Office will assist the G-8 with Goal 4.

h. The Office of the Provost Marshal General will assist the G-3/5/7 with Goals 1, 4, 5, and 6.

i. The Office of The Surgeon General will assist the G-3/5/7 with Goals 1, 2, 3, 5, and 6.

j. The Assistant Chief of Staff for Installation Management (ACSIM) and the Assistant Secretary of the Army (Installations and Environment) will assist the G-3/5/7 and G-8 with all Goals.

k. The US Army Training and Doctrine Command will assist the G-3/5/7 with Goals 3 and 6.

Appendix E

Army Protection Policy Guidance

ANNEX – PROTECTION GOALS AND OBJECTIVES

Goal 1. Enhance integration and coordination of all protection-related activities.
Ensuring Army-wide protection efforts receive the appropriate guidance and direction from one central source is key to providing senior leadership with the requisite situational awareness to deconflict efforts, reduce duplication, prioritize areas of focus, and approve new initiatives.

Objective 1: Establish an Army Staff (ARSTAF) integrator for protection.
Objective 2: Establish an Army oversight board for protection.
Objective 3: Develop capstone protection policy.
Objective 4: Ensure routine flow of protection-related information.
Objective 5: Institute a linkage with Joint Staff protection initiatives and funding streams.

Goal 2. Provide strategic guidance to focus and deconflict ongoing and future protection efforts.
Integrating protection into the Army's guiding strategic documents will ensure that this strategy's principles are addressed and provide the broad guidance necessary to bring focus to a key component of the Army's ongoing transformation and war on terror.

Objective: Integrate Army protection expectations into strategic documents.

Goal 3. Ensure the integration of force capabilities.
Developing centrally coordinated and effective protection-oriented capabilities is necessary to respond rapidly to operational needs while simultaneously ensuring effective use of available resources.

Objective 1: Improve ARSTAF response to protection needs.
Objective 2: Publish Army guidance to coordinate capabilities development.

Goal 4. Provide a common operational picture (COP) for protection-related funding.
Providing a Protection COP for senior leaders to influence and direct protection-related funding actions across program and budget years will significantly improve Headquarters, Department of the Army oversight of all Army protection programming and budgeting efforts.

Objective 1: Establish periodic review of protection requirements and funding across all Program Evaluation Groups.
Objective 2: Develop routine crosswalk of short-term funding.
Objective 3: Conduct periodic execution reviews of protection funding.

Appendix E

Army Protection Policy Guidance

ANNEX - PROTECTION GOALS AND OBJECTIVES

Goal 5. Set protection guidelines for the application of risk management principles.
Identifying appropriate metrics and using existing reporting systems to measure performance of protection readiness across the institutional and operational Army while simultaneously reducing the administrative burden on reporting/assessed organizations will improve senior leadership's ability to manage Service wide risk.

Objective 1: Identify metrics for evaluating success of Army protection efforts.
Objective 2: Establish a protection reporting system.
Objective 3: Consolidate and integrate related functional assessments to effect a holistic protection assessment.

Goal 6. Establish protection priorities to guide a concerted effort across the Army.
Executing this strategy will require a deliberate process to identify the specific programs, related functions, and funding streams that compose and support Army protection.

Objective 1: Establish protection functions and associated programs.
Objective 2: Embed the protection concept in Army procedures and planning.

Appendix F (G-34 Protection Division Concept) to Fort Hood Army Internal Review Team Final Report

One option to address shortfalls in how we implement policy, prioritize requirements and program necessary resources to meet current and emerging protection requirements is to establish a G-34. The purpose of a G-34 for protection organization would be to establish a coordinating staff to synchronize protection related functions into a coherent program maximizing safety and security of Soldiers, Civilians, Families, infrastructure and information. G-34 would provide unity of effort to disparate protection programs, currently operating along independent lines of operation. G-34 would serve as the OPR to prioritize protection related requirements and funding to ensure concerted actions against threats affecting Army resiliency. The G-34 would coordinate protection issues with similarly organized organizations with the JS, other Services and the combatant commands.

The G-3/5/7 and senior commanders are responsible for protection, yet do not control or have sufficient authority to influence protection functions and funding. In the current HQDA organization, G-3/5/7 has neither funding authority nor control over the following protection functional areas:

- Antiterrorism (FY10 - $27 Million).
- Fire and Emergency Services (FY10 - $218 Million).
- Force Health Protection, High-Risk Personnel, Information Assurance, Law Enforcement (FY10 - $163 Million).
- Physical Security and Safety (FY10 - $471 Million).

The G-3/5/7 "remains the functional proponent for Army FP" per General Orders No. 9, dated 26 September 2003. As the Army proponent for protection, G-3/5/7 controls funding for only five of the 13 protection functional areas. The protection functional areas controlled by G-3/5/7 are the EM Program, Computer Network Defense, Continuity of Operations Program (COOP), Critical Infrastructure Risk Management and Operations Security. Protection related functions are spread over 90 different MDEPs across the six PEGs limiting unity of effort, creating gaps in C2 and leading to disjointed protection efforts. The table below shows the current protection functional areas structure across the MDEPs and PEGs.

Program or Functional Area (Protection 13)	Proponent	PEG	MDEP
Emergency Management Program (EM) (FY10-$17 M)	G-3/5/7	II	Visibility Installation Protection Program
Computer Network Defense (CND)	G-3/5/7	TT	Information Operations
Continuity of Operations Program (COOP)	G-3/5/7	OO/ TT	XMGH/ MU2B
Critical Infrastructure Risk Management (CIRM)	G-3/5/7	OO	XMGH
Operations Security	G-3/5/7	TT	Information Operations
Antiterrorism (AT) (FY10-$27 M)	G-3/5/7 *See note below	II	Antiterrorism (VTER)

Program or Functional Area (Protection 13)	Proponent	PEG	MDEP
Fire and Emergency Services (F&ES) (FY10-$218 M)	ACSIM	II	Public Works Facilities Operations (QDPW-P)
Force Health Protection	OTSG	MM, EE, TT, OO, SS	Multiple MDEPs and Defense Health Program Funding
High-Risk Personnel (HRP)	OPMG	II	Antiterrorism (VTER)
Information Assurance (IA)	CIO/G-6	II	HQDA Command and Control
Law Enforcement (FY10-$163 M)	OPMG	II	Law Enforcement, Physical Security, Plans, Training and Mobilization Activities (QLPR)
Physical Security (PS) (FY10-$471 M)	OPMG	II	Physical Security Matters (QPSM)
Safety (S)	Office of Admin Assistant(OAA)	OO	The Army Safety Center

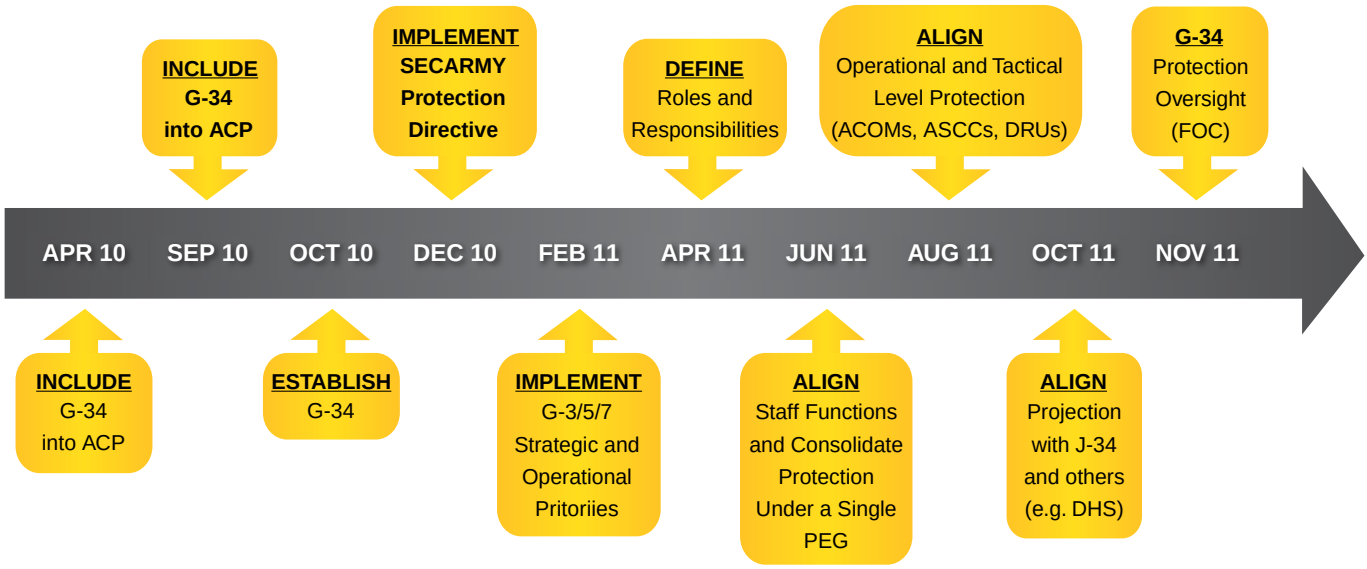
*** Note:** While G-3/5/7 is the proponent, OPMG is the MDEP manager and controls funding and distribution of AT resources.

AAA noted "The Army aligned functional responsibilities for FP with appropriate organizations. However, responsibility gaps existed that could detract from unity of effort, C2 and streamlined operations." (Report A-2007-0177-FFD - Roles and Responsibilities for FP - 30 July 2007) AAA stated that Army needed to "redefine or establish new MDEPs to better align resources." Secretary of the Army Directive 2008-02, Army Protection, indicated "The goal of this directive is to synchronize all Army protection-related functions into a coherent program." Based on the DoD Independent Review Panel, it is likely that OSD will assign a senior level individual, or steering group, responsibility to integrate protection policy and coordinate efforts within the J-34. As such, Army should organize a G-34 to align and prioritize resources so that authorities, roles and responsibilities do not remain "stovepiped," resulting in unfocused spending, inefficient communication and ineffective execution.

The Fort Hood AIRT's recommendation is to fully develop and implement this solution to coordinate and synchronize all Army protection functions. The G-34 will enable the G-3/5/7 to meet the responsibilities specified in Army Directive 2008-02. Without this capability, there is no staff element dedicated to integrate and synchronize over 90 MDEPs, 6 PEGs and numerous ARs that govern Protection functions.

The figure below represents G-34 goals as outlined by Army Directive 2008-02.

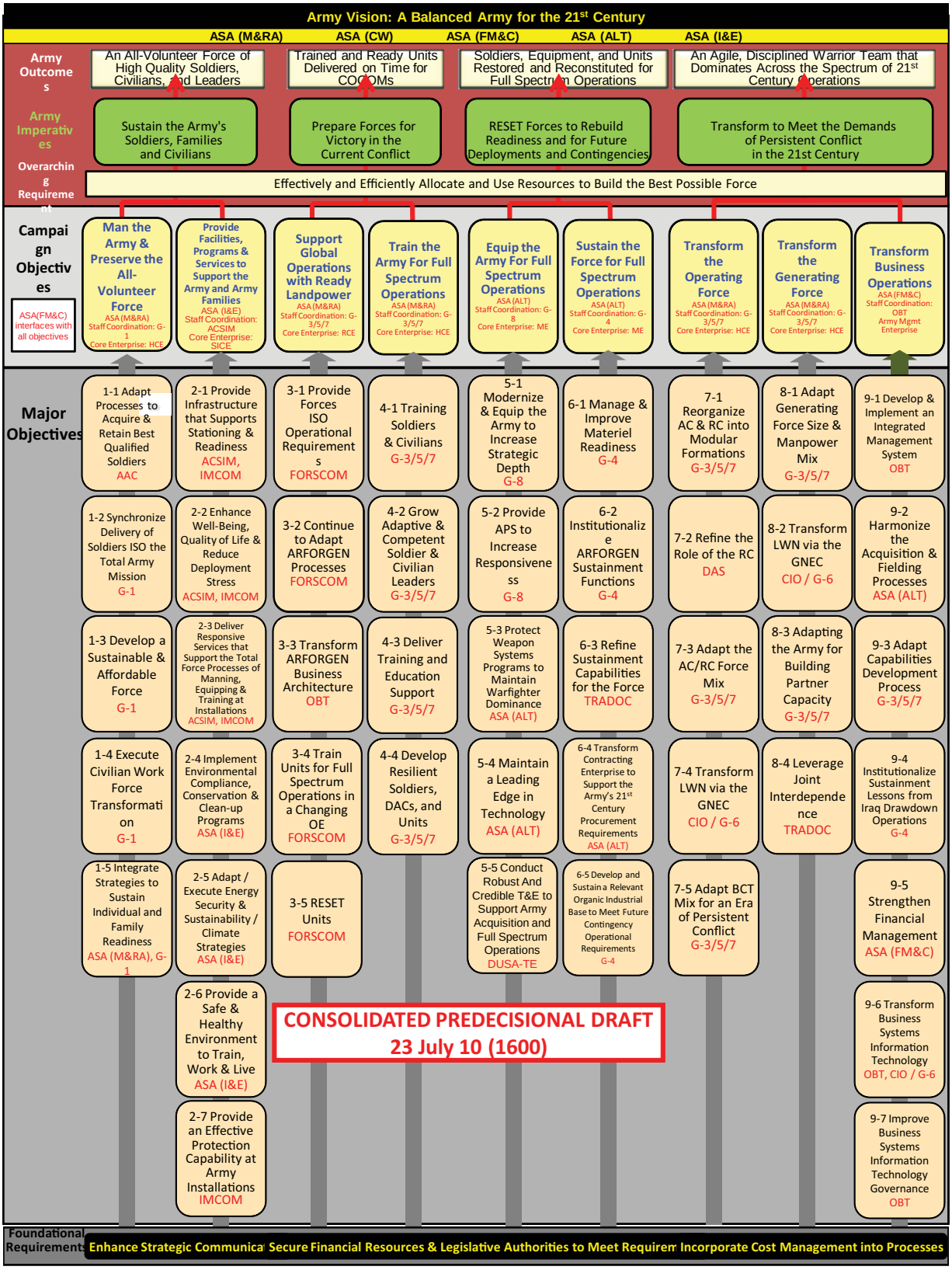
The projected timeline to establish a fully functional G-34 is below.



The G-34 will accomplish the following tasks for the Army:

- Implement Secretary of the Army Directive 2008-02.
- Implement strategic and operational priorities established by the G-3/5/7.
- Define Protection-related roles and responsibilities.
- Align Army Staff functions and ensure consolidation of Protection and Protection-related requirements under a single functional PEG.
- Align strategic, operational and tactical level protection efforts of ACOMs, ASCCs and DRUs with HQDA policy and priorities.
- Align Protection efforts with JSs, other Services and federal agencies such as Department of Homeland Security.

Appendix G (Army Campaign Plan Outcomes and Objectives) to Fort Hood Army Internal Review Team Report



Appendix H (Explanation of the Recommendation Database and Survey Results) to Fort Hood Army Internal Review Team Report

A. Overview. The Fort Hood AIRT developed two separate IT products to better analyze and assess the DoD Independent Review Panel's Findings and Recommendations and to determine the appropriate Army action.

1) Fort Hood AIRT Database Management System: The Fort Hood AIRT Database System is a relational database made of three major tables and several lookup tables. The major data tables are Findings, Recommendations and Actions. Access the database through the Fort Hood AIRT website.

2) Fort Hood AIRT Web Site:

a) The Fort Hood AIRT Web Site is a graphical user interface. The development of this tool enabled the Fort Hood AIRT to manage and track the status and supporting data of the 79 recommendations resulting from the DoD Independent Review Panel. This tool provides team members, supporting team members and selected installation commanders the ability to efficiently collaborate and share information on a real time basis.

b) The home page of the website displays the main links to the internal data relating to the findings and recommendations. The major tabs are Findings, Dashboard, Reports and Survey. The findings tab allows you to view and update the 41 findings as well as to look at the resulting recommendations. You may further look at the actions taken by the lead agencies and the review team.

c) The Dashboard tab displays a graphical view (Pie Charts) of the 79 recommendations. The Pie Charts depicts the status (red, amber and green) of the recommendations. You may opt to display the status by Major Areas, Lead Agency, PEG and Reviewer.

d) The reports tab summarizes the team's input in five report formats. The Summary, Recommendation, Actions, Agencies and Ratings reports are available beneath the reports tab. The"Ratings" report list the 79 recommendations and the number of ratings for each recommendation.

e) The survey tab allowed selected CONUS Installations/Garrison the opportunity to rate the 79 recommendations. The data collected became the tool for the team to determine the importance of the 79 recommendations.

f) Individuals having permissions to use this tool can find the website on URL: https://secureappcac.hqda.pentagon.mil/fthood/. For access to the website contact: OAACommunicationsPOC@conus.army.mil. Anyone needing access to this site will contact this office.

g) Recommendations and Actions. Personnel, FP, Information Sharing, Emergency Response and Health Affairs are the five major areas of the 79 recommendations. When selecting a particular finding, you may further look at the related recommendations and actions.

B. Installation Commander Survey. Approximately 105 AMC and IMCOM Commanders were solicited to participate in a survey to confirm or dispute the value the DoD review team placed on the 79 recommendations. Eighty-four (84) Commanders completed a survey where they rated the seventy-nine

(79) OSD recommendations from 1 to 10. A rating of 10 indicated high impact to their installation, if implemented, and a rating of 1 indicated little or no impact to their installation. Eighty-four (84) installations responded to the survey. Note that OSD did not assign a value to 26 of the 79 recommendations. Army installation commanders rated all 79 OSD recommendations. Recommendations not noted below received a "medium impact" rating from Army installations. The results, along with OSD's rating, are as follows:

Personnel	Installation Commanders	OSD
2.2.A	High Impact	Medium Impact
2.3.A	Low Impact	Not Rated
2.10.A	High Impact	Not Rated
Force Protection		
3.9.A	High Impact	High Impact
3.9.B	High Impact	High Impact
3.9.C	High Impact	Medium Impact
Emergency Response		
4.3.A	High Impact	High Impact
4.3.B	High Impact	Not Rated
4.3.C	High Impact	Not Rated
4.4.A	High Impact	High Impact
4.5.A	High Impact	Medium Impact
Information Sharing		
3.B	Low Impact	Not Rated
3.3.C	Low Impact	Not Rated
3.6.A	High Impact	High Impact
Health Affairs		
5.4.A	Low Impact	High Impact

Appendix I (Strategic Communications Plan) to Fort Hood Army Internal Review Team Report

NOTE: This Strategic Communication Plan supports the Fort Hood AIRT Report to the OSD. This report addresses the 79 issues outlined in the Former Secretary of the Army Togo West and Retired Admiral Vernon Clark January 2010 DOD Independent Review of the Fort Hood Shootings. The team's goal is to assess the Army's ability below the headquarters level to identify internal threats, FP and emergency response programs, policies and procedures.

A. Situation.

1) Strategic Context.

a) America's Army continues to answer the Nation's call, as it has since its birth 235 years ago. Today our Army is fighting two wars, assisting other nations as they build their own security capacity, supporting civil authorities at home, helping the peoples around the globe rebuild after a devastating natural disasters and preparing to deter and defeat new threats. The Army's Soldiers, Civilians and Families faithfully shoulder the load that our Nation asks of them.

b) The Army has operated at a demanding pace for the last eight years, and has met each challenge. Against that backdrop, Soldiers continue to meet the wartime requirements of our Nation. In an era of persistent conflict, commanders and leaders at all levels must protect the safety and security of our service members and their families, as well as Army facilities. Commanders, particularly at the installation level, must continue to identify, assess and counter threats to Soldiers, Civilians and their Families. The Army has a proud history of providing safe, threat-free environments for Soldiers and their Families to live and train. The safety and security of Soldiers, Civilians and Family members remains the Army's number one priority.

2) Issue.

a) The Army established the Fort Hood AIRT as a result of the 5 November 2009 shootings at Fort Hood, TX. The team is a task force convened by the VCSA. The team's charter is to (1) Conduct a review and assessment of the Army's ability to identify internal threats, FP and emergency response then submit a report of the team's findings to the ASD(HD&ASA) through the VCSA; (2) review and develop an implementation plan for those findings and recommendations published by the DoD Independent Review Panel in their January 2010 report; and (3) recommend additional actions as deemed appropriate.

b) To date, the Fort Hood AIRT has focused on assessing how DOD and Army-level policies enable installation-level commanders to detect, prevent, respond and recover from a Fort Hood like incident. To this end, the Fort Hood AIRT surveyed 84 current installation commanders and asked them to rank the 79 recommendations drawn from the report of the DOD Independent Review Panel on Fort Hood in terms of the perceived value each could bring to enhancing FP. The Fort Hood AIRT also conducted site visits known as "Deep Dives" of 17 installations worldwide to identify the challenges faced by our installation commanders and the best practices they have developed to address those challenges. Additionally, MG Robert Radin, the leader of the Fort Hood AIRT, attended an annual installation commanders' conference and conducted a panel discussion session with 10 installation level commanders representing Army installations worldwide. The Fort Hood AIRT efforts, to date, have yielded the following specific findings:

- Installation-level commanders rated 11 of the 79 recommendations in the DOD Independent Review Panel report as high impact, 64 as medium and 4 as low impact. This prioritization will aid commanders in determining which recommendations to incorporate first as they respond to the report's findings.
- The Army has already implemented 21 of the 79 DOD Independent Review Panel recommendations.
- The Army has identified and implemented 10 "Quick Wins" – programs and processes that were not specifically called out in the 79 recommendations of the DOD Independent Review Panel report.
- The Army has developed rough cost estimates for many of the DOD Panel's recommendations and continues in its efforts to complete a comprehensive cost estimate report.

c) Taken individually, no single action would have prevented the tragedy at Fort Hood. However, in the aggregate, the initiatives outlined by the Army's internal review team will significantly improve the Army's ability to mitigate internal threats, ensure FP, enable emergency response and provide care for the victims and families.

3) Background/Discussion.

a) On 19 November 2009, the Secretary of Defense announced a DOD-wide installation security review. The review, in response to the shooting incident at Fort Hood, TX on 5 November 2009, would assess the safety and security of DOD employees and their families. Secretary Togo West and retired Admiral Vernon Clark completed the DOD Independent Review in January 2010.

b) On 1 March 2010, the Vice Chief of Staff, Army, appointed MG Robert Radin to stand-up and lead the Fort Hood AIRT. On 19 April 2010, the Vice Chief of Staff, Army, signed the Fort Hood AIRT's charter and issued a Fort Hood Army Follow-On Internal Review Tasking Memo, which directed the Fort Hood AIRT to conduct analyses and develop implementation plans for the recommendations of the DOD Independent Review Panel and to identify additional recommendations if needed.

c) The primary members of the Fort Hood AIRT are senior representatives (O-6 or civilian equivalent) from key HQDA staff elements and proponent stakeholders. Primary team members are assigned full-time to the Fort Hood AIRT. The team will terminate once it submits the Fort Hood Internal Review Team Report to the Vice Chief of Staff, Army. Army efforts will not end here. Approved recommendations will be tracked as part of the Army Campaign Plan.

4) Audiences. Primary audiences are OSD, Congress (SASC, HASC), victims of the shooting, Soldiers, Family members and Army Civilians, Guard and Reserve personnel.

5) Audience Analysis.

a) OSD established an independent review panel following the shooting at Fort Hood. That panel made numerous findings and the Fort Hood AIRT was created to explore those findings and make recommendations at the direction of the Secretary of Defense and Secretary of the Army.

b) Members of Congress have made several requests for information from the Army regarding the Fort Hood shooting and the alleged perpetrator. Much of the information requested has not been released because it would compromise the trail of the alleged perpetrator.

Senior leaders may be called to testify about the team's results.

c) Soldiers will take a keen interest in the Fort Hood AIRT's findings with respect any changes in the promotion and personnel policies. Given that Soldiers are the primary targets in incidents like this, it will be important to communicate the team's purpose to find ways to prevent tragedies like this in the future, and how recommendations will affect them in the future. It is also important to communicate that senior leadership takes the FP and security seriously.

d) Like their Soldiers, Family Members are concerned with FP and security not only for their Soldier but for themselves and their children. They will be concerned with insuring that internal threats are identified, in addition to knowing about the actual recommendations implemented as a result of the team's report.

e) It will be important to emphasize to Civilians that they are also included in this report. Often many Civilians pay little attention to new training and policy initiatives, feeling they do not really apply to them. It will be important to emphasize the team's findings may affect their professional responsibilities.

B Mission.

1) **Purpose:** The purpose of this Strategic Communication initiative is to inform and educate both internal and external audiences on the goals and mission of the Fort Hood AIRT.

2) **Desired Effects of Communications Campaign.**

a) Soldiers and leaders can articulate the mission and goals of the Fort Hood AIRT.

b) Audiences share Army's view of the Fort Hood AIRT.

c) Audiences understand the importance to Fort Hood AIRT.

d) Audiences understand risk of failure to fully incorporate the recommendations of Fort Hood AIRT.

e) Tonality (positive/negative/neutral) of national media stories on Fort Hood AIRT initiative.

3) **Overarching communication strategy:** The communication strategy is active. The main focus is on OSD, Soldiers and Congress. Commanders' conferences, installation town hall meetings, media releases/interviews, social media activities, Stand-To, Soldier Radio Television, Army News, briefings to Members of Congress and professional articles will be the vehicles used to communicate with our audiences.

4) **Overarching Theme:** The safety and security of Soldiers, Civilians and Family members is the Army's number one priority. Messages:

- The Fort Hood shooting is a tragedy that the Army has taken very seriously to ensure accountability and to prevent any future incidents.
- Our top priority remains to care for our Soldiers and their Families affected by this tragedy.
- The entire Army Family – Soldier, Family Member, Civilian, Retiree or Veteran – responded rapidly to Fort Hood and continued the long tradition of 'taking care of our own' in times of crisis and need.

- The Fort Hood AIRT is a task force convened by the VCSA as a result of the 5 November 2009 shootings at Fort Hood, TX. The team:
  - Conducted a review and assessment of the Army's ability to identify internal threats, FP and emergency response then submitted a report of the team's findings to the ASD(HD&ASA)
  - Reviewed and developed an implementation plan for those findings and recommendations published by the DoD Independent Review Panel in their January 2010 report.
  - Recommended additional actions as deemed appropriate.
- The Fort Hood AIRT team has come up with 10 "Quick wins," (immediate fixes) as it explores the 79 recommendations of the DoD report on the Fort Hood incident. These 10 "Quick Wins are "over and above" the 79 recommendations proposed by the DOD team.

C. Execution Matrix. RE-EVALUATION TIMELINE: Quarterly

DATE	MESSAGES	ENGAGEMENTS
28 June 10	The Fort Hood shooting is a tragedy and the Army has taken measures to mitigate the risk of any future incidents occurring. Our top priority remains to care for our Soldiers and their Families affected by this tragedy.	Stand To Focus Article
25-27 Oct 10	No Change	Professional Organization Symposiums, Washington, D.C.
TBD	The Fort Hood AIRT conducted a review and assessment of the Army's ability to identify internal threats, FP and emergency response and submitted a report of the team's findings to the ASD(HD&ASA) Discuss details of report	Hill testimony

ANNEX (Talking Points) to Appendix I (Strategic Communications Plan) to Fort Hood Army Internal Review Team Report

- The Army has a proud history of providing safe, threat-free environments for Soldiers and their Families to live and train. The safety and security of Soldiers, Civilians and Family members remains the Army's number one priority.
- The Fort Hood AIRT's goal is to assess the Army's ability below the headquarters level to identify internal threats, FP and emergency response programs, policies and procedures.
- On 1 March 2010, the Vice Chief of Staff, Army, appointed MG Robert Radin to stand-up and lead the Fort Hood AIRT and directed the team to conduct analyses and develop implementation plans for the recommendations of the DOD Independent Review Panel and to identify additional recommendations if needed.

- Fort Hood AIRT team members conducted site visits known as "deep dives" of 17 Army installations worldwide. During these visits members met with installation commanders and their staffs to discuss their threat assessment and FP programs. Results of these visits are compiled for inclusion into the final report.
- Taken individually, no single action would have prevented the tragedy at Fort Hood. However, in the aggregate, the initiatives outlined by the Army's internal review team will significantly improve the Army's ability to mitigate internal threats, ensure FP, enable emergency response and provide care for the victims and families.
- The Fort Hood AIRT has identified 10 "Quick Wins" during its visits to installations and coordination with various HQDA agencies. "Quick Wins" are programs, policies and/or processes easily instituted that will aid the Army identifying internal threats, enhance FP and emergency response programs. The "Quick Wins" are broken out into four categories, Detect, Prevent/Preclude, Respond and Recover. They are:

DETECT

- ARMY IMPLEMENTATION OF COUNTERINTELLIGENCE REPORTING SYSTEM. The G-2 Staff in conjunction with the G-6 staff created a CI reporting link for both AKO and AKO-S. The link will allow AKO users to submit tips about suspicious behavior to G-2 investigators. Both links are now operational.
- ARMY IMPLEMENTATION OF IWATCH (TERRORISM WATCH PROGRAM). The Army will implement a new program similar to a neighborhood watch program that will teach members of the Army community to recognize and report suspicious behavior. The program is slated to begin 1 August 2010.
- REVISION OF AR 381-12, Threat Awareness and Reporting. The Army is revising existing threat reporting training to include more robust reporting requirements and the activation to the new AKO reporting sites. This training is in the final stages of review.

PREVENT/PRECLUDE

- ARMY EMERGENCY MANAGEMENT PLANNERS COURSE AT FORT LEONARD WOOD. The Army has begun sending its EM professionals to specialized training at Fort Leonard Wood. The training is being coordinated by Army training and combat planners.

RESPOND

- ACTIVE SHOOTER TRAINING WITHIN THE ARMY LAW ENFORCEMENT COMMUNITY. The Army had expanded and refined active-shooter training for the Army law enforcement community. This includes increased training for new military police officers and annual recertification for currently servicing military and civilian police officers.
- LAW ENFORCEMENT USE OF JACKETED HOLLOW POINT AMMUNITION. The Army law enforcement community authorized and began issuing jacketed hollow point ammunition as of 30 April. This type of ammunition is less likely pass through multiple objects and reduces the possibility of collateral damage.

- ARMY EMERGENCY MANAGEMENT PROGRAM. The Army will begin briefing general officers and senior commanders at the Army Management Staff College to better acquaint them with the Army's EM plan to ensure that senior commanders have the tools they need prior to an emergency occurring.
- INSTALLATION EMERGENCY CAMPAIGN PLAN (ICP). IMCOM HQ has begun to require installations to develop EM plans that are NIMS compliant. This will make the plans interoperable with local, county and state emergency personal systems.
- ARMY EMERGENCY MANAGEMENT "CERTIFICATION" WORKSHOP, JULY 2010. The army will be certifying EM officials in the NIMS to assist the installations in creating emergency plans that are compliant with those standards. Installations are required to be initially compliant by 2011 and fully compliant by 2014.

RECOVER

- IMPLEMENTATION OF THE TRAUMATIC EVENT MANAGEMENT (TEM) COURSE. The Army started a new training program to train mental health providers and chaplains in TEM. The initial pilot program has already been completed with six more classes planned for different installations across the Army.

  The team will terminate once it submits the Fort Hood Internal Review Team Report to the Vice Chief of Staff, Army. Army efforts will not end here. Approved recommendations will be tracked as part of the Army Campaign Plan.

Appendix J (References) to Fort Hood Army Internal Review Team Report

"Protecting the Force: Lessons from Fort Hood." Report of the DoD Independent Review Panel, January 2010.

Secretary of Defense Memorandum, Subject: Interim Recommendations of the Fort Hood Follow-on Review, 12 April 2010.

DoD 6025.18R Standard: Uses and Disclosures for Specialized Government Functions, 24 January 2003

DoD 6025.13R Military Health System Clinical Quality Assurance Program, under current revision

DoDI 5240.6 CI Awareness, Briefing and Reporting Programs

DoDI 5240.mm Counterintelligence (CI) Activities in Cyberspace

DoDI 6490.1 Mental Health Evaluation of Members of the Armed Forces, under current revision

DoDI 6490.4 Requirements for Mental Health Evaluation of Members of the Armed Forces, under current revision

DODD 6490.1 Mental Health Evaluations of Members of the Armed Services

DoDI 6490.4 Requirements for Mental health Evaluations of Members of the Armed Forces

DoDI 6490.07 Deployment- Limiting medical Conditions for Service Members and DoD Civilian Employees

DoDD 6490.1 Mental Health Evaluations of Members of the Armed Services

DoDI 6490.4 Requirements for Mental Health Evaluations of Members of the Armed Forces

DoDI 5210.90 Minimum Training, Certification and Physical Fitness Standards for Civilian Police and Security Guards (CP/SGs) in the Department of Defense 7/9/2007

Directive-Type Memorandum (DTM) 09-006- revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel, 2 July 2009.

Directive-Type Memorandum (DTM) 09-006, Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health to Military Personnel, 2 July 2009

JP 2-0 Joint Intelligence 6/22/2007

AR 25-1 Information Assurance, Rapid Action Revision 3/23/2009

AR 40-1 Composition, Mission, and Functions of the Army Medical Department, 7/11/1983

AR 40-66 Medical Record Administration and Health Care Documentation, Rapid Action Revision 2, 01/04/2010

AR 40-68 Clinical Quality Management 5/22/2009

AR 165-1 Army Chaplain Corps Activities, 12/3/2009

AR 190-11 Physical Security of Arms, Ammunition and Explosives 11/15/2006

AR 190-12 Military Working Dog Program 6/4/2007

AR 190-13 The Army Physical Security Program 9/30/1993

AR 190-14 Carrying of Firearms and Use of Force for Law Enforcement and Security Duties 3/12/1993

AR 190-56 The Army Civilian Police and Security Guard Program 10/15/2009

AR 190-58 Personal Security 3/22/1989

AR 195-2 Criminal Investigation Activities 5/15/2009

AR 380-13 Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations 9/13/1974

AR 381-12 Subversion and Espionage Directed Against the Army (SAEDA) 1/15/1993

AR 381-20 The Army Counterintelligence Program, 6/25/2010

AR 525-13 Antiterrorism, 9/11/2008

AR 525-27 Army Emergency Management Program, 3/13/2009

FM 3-19.30 Physical Security 1/8/2001

FM 4-02.51 Combat and Operational Stress Control, 26 July 2006

FM 6-22.5 Combat and Operational Stress Control Manual for Leaders and Soldiers, 18 March 2009

ALARACT 049 2010 Guidance for Physical Access Control for Army Installations (DTG: 191713Z FEB 10

ALARACT 135/2010 Authorization to Use Jacketed Hollow Point (JHP) Ammunition from Army Inventory for Law Enforcement (LE) on Army Installations DTG: P 071051Z MAY 10

ALARACT 049/2010 – Guidance for Physical Access Control for Army Installations DTG 191713Z FEB 10

ALARACT 025/2010 - HQDA EXORD 087-10 ISO Annual Military Police Law Enforcement Training and Certification

Training Support Package 191-AS-0001 3/1/2010 - Active Shooter Response (ASR)

Army Audit Agency report, A-2007-0177-FFD, “Roles and Responsibilities for Force Protection,” 30 Jul 2007.

Appendix K (Fort Hood Army Internal Review Team Membership) to Fort Hood Army Internal Review Team Report

The Fort Hood Army Internal Review Team full-time members:

Team Lead Major General Robert Radin

Chief of Staff Colonel Allen Kiefer

Executive Officers Major Gabe Pryor/ Major Michael Lalor

ASA(M&RA) Leads Colonel BJ Constantine/ Colonel Kerk Brown/ Lieutenant Colonel Laura Wages

G-2 Lead Colonel Jim Stuteville

G-3/5/7 Lead Colonel John Domenech

ACSIM Lead Colonel Regina Grant

OPMG Lead Lieutenant Colonel Bruce Barker

OTSG Leads Colonel Jim Daniels/ Lieutenant Colonel Gary McKay

OCCH Lead CH(Colonel) Michael Hoyt

CAA Lead Mr. Bill Wright

Legal Counsel Major Kirsten Dowdy/ Major Dana Venneman

Contributing Members:

ASA(FM&C) Mr. James Bliss

G-6 Mr. Gus Ortiz

G-8 Mr. Ed Molnar

OCLL Lieutenant Colonel Dean Vlahopoulos

OCPA Mr. Emerson Pittman

AAA Mr. Craig Emerson

Appendix L (Acknowledgements) to Fort Hood Army Internal Review Team Report

The Fort Hood AIRT gratefully acknowledges the assistance and support of the following organizations and people, without whom our mission could not have been accomplished.

Office of the Administrative Assistant to the Secretary of the Army

- Ms. Joyce Morrow
- Mr. Steve Redmond
- Mr. David Cleveland
- MSG Dale Barlow

Office of the General Counsel

- Ms. Stephanie Barna
- Mr. Daniel McCallum
- Mr. Ronald Buchholz

Directorate of Army Information Management Support Center (IMCEN)

- Mr. Timothy Devine
- Ms. Victoria Tate
- Mr. George Krenik
- Mr. Maurice Pierce
- Ms. Mary Caneva
- Ms. Lola Ferguson
- Ms. Kelsey Bishop
- Mr. Frank Fang
- Mr. Shaun Rowan
- Ms. Mimi Tadesse
- Mr. Dan Ritz
- Ms. Dorothy Jones

Office of the Vice Director of the Army Staff

- Mr. Jim Gunlicks
- Mr. Ed Bready
- Ms. Heather Drake
- Ms. Regina Thompson
- Ms. Rachel McLeod
- SGT Derek Kissos

Appendix M (Acronyms) to Fort Hood Army Internal Review Team Report

AAA	Army Audit Agency
ACOMs	Army Commands
ACS	Army Community Service
ACSIM	Assistant Chief of Staff, Installation Management
AIES	Army Investigative Enterprise Solution
AIRT	Army Internal Review Team
ALARACT	All Army Activities (message)
ALI	Automatic Location Identification
AMC	Army Materiel Command
AMEDD	Army Medical Department
ANI	Automatic Number Identification
AOR	Area of Responsibility
AR	Army Regulation
ARNORTH	United States Army North
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ASA(FM&C)	Assistant Secretary of the Army (Financial Management & Comptroller)
ASA(I&E)	Assistant Secretary of the Army (Installations & Environment)
ASA(M&RA)	Assistant Secretary of the Army (Manpower & Reserve Affairs)
ASCC	Army Service Component Command
ASD(HD&ASA)	Assistant Secretary of Defense (Homeland Defense & Americas' Security Affairs
ASR	Active Shooter Response
ATMU	Army Threat Management Unit
BRP	Budget Requirements and Programming Board process
C2	Command and Control
CAA	Center for Army Analysis
CAD	Computer Aided Dispatch
CBA	Cost-Benefit Analysis
CCF	Central Clearance Facility
CI	Counter-intelligence

CID	U.S. Army Criminal Investigation Command
CIO/G-6	Chief Information Officer/G-6
CIRM	Critical Infrastructure Risk Management
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CJIS	Criminal Justice Information System
CONUS	Continental United States
COP	Common Operating Picture
COOP	Continuity of Operations Program
CRB	Crisis Response Battalion
CSF	Comprehensive Soldier Fitness
CSG	Contract Security Guard
CT	Counter-terrorism
DA PAM	Department of the Army Pamphlet
DACP	Department of the Army Civilian Police
DASG	Department of the Army Security Guard
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoDI	Department of Defense Instruction
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities
DRU	Direct Reporting Unit
DSB	Defense Science Board
E911	Enhanced 911
EM	Emergency Management
EMSG	Emergency Management Steering Group
EMWG	Emergency Management Working Group
EOC	Emergency Operations Center
FAC	Family Assistance Center
FBI	Federal Bureau of Investigation
FM	Field Manual
FOC	Full Operational Capability
FP	Force Protection

FPCON	Force Protection Condition
FY	Fiscal Year
GIS	Geographical Information System
GPS	Global Positioning System
HQDA	Headquarters, Department of the Army
HSPD-12	Homeland Security Presidential Directive 12
IEM	Installation Emergency Management
IFPEX	Installation Force Protection Exercises
II PEG	Installation Program Evaluation Group
IMCOM	Installation Management Command
INSCOM	US Army Intelligence and Security Command
IOC	Initial Operational Capability
IT	Information Technology
JITF-CT	Joint Intelligence Task Force – Counter Terrorism
JS	Joint Staff
JTTF	Joint Terrorism Task Force
MAA	Mutual Aid Agreement
MAVNI	Military Accessions Vital to National Interest
MDEP	Management Decision Package
MEDCOM	US Army Medical Command
MILCON	Military Construction
MOU	Memorandum of Understanding
MP	Military Police
MWN	Mass Warning and Notification
NACI	National Agency Check with Written Inquiries
NCIC	National Crime Information Center
NGB	National Guard Bureau
NIMS	National Incident Management System
NJSSRT	National Joint Security and Suitability Reform Team
NMCC	National Military Command Center
NORTHCOM	U.S. Northern Command
NRF	National Response Framework

NTMU	Navy Threat Management Unit
OCCH	Office of the Chief of Chaplains
OCPA	Office of the Chief of Public Affairs
OGC	Office of General Counsel
OPM	Office of Personnel Management
OPMG	Office of the Provost Marshal General
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
OTJAG	Office of the Judge Advocate General
OTSG	Office of the Surgeon General
PEG	Program Evaluation Group
PM	Provost Marshal
SAEDA	Subversion and Espionage Directed Against the Army
SAR	Suspicious Activity Reporting
SICE	Services and Infrastructure Core Enterprise
SIPRNET	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SOP	Standard Operating Procedure
TEM	Traumatic Event Management
TRADOC	U.S. Army Training and Doctrine Command
TSP	Training Support Package
USACHCS	United States Army Chaplain Center and School
USAREUR	United States Army Europe
USAG	United States Army Garrison
USAMPS	United States Army Military Police School
USD(I)	Under Secretary of Defense (Intelligence)
VCSA	Vice Chief of Staff, Army
VIPP	Visibility Installation Protection Program

This page has been left blank intentionally

5 MAJOR AREAS:

PERSONNEL

INFORMATION SHARING

FORCE PROTECTION

INSTALLATION EMERGENCY RESPONSE

HEALTH AFFAIRS

Protecting our Army community

U.S. ARMY

FORT HOOD ARMY INTERNAL REVIEW TEAM: FINAL REPORT