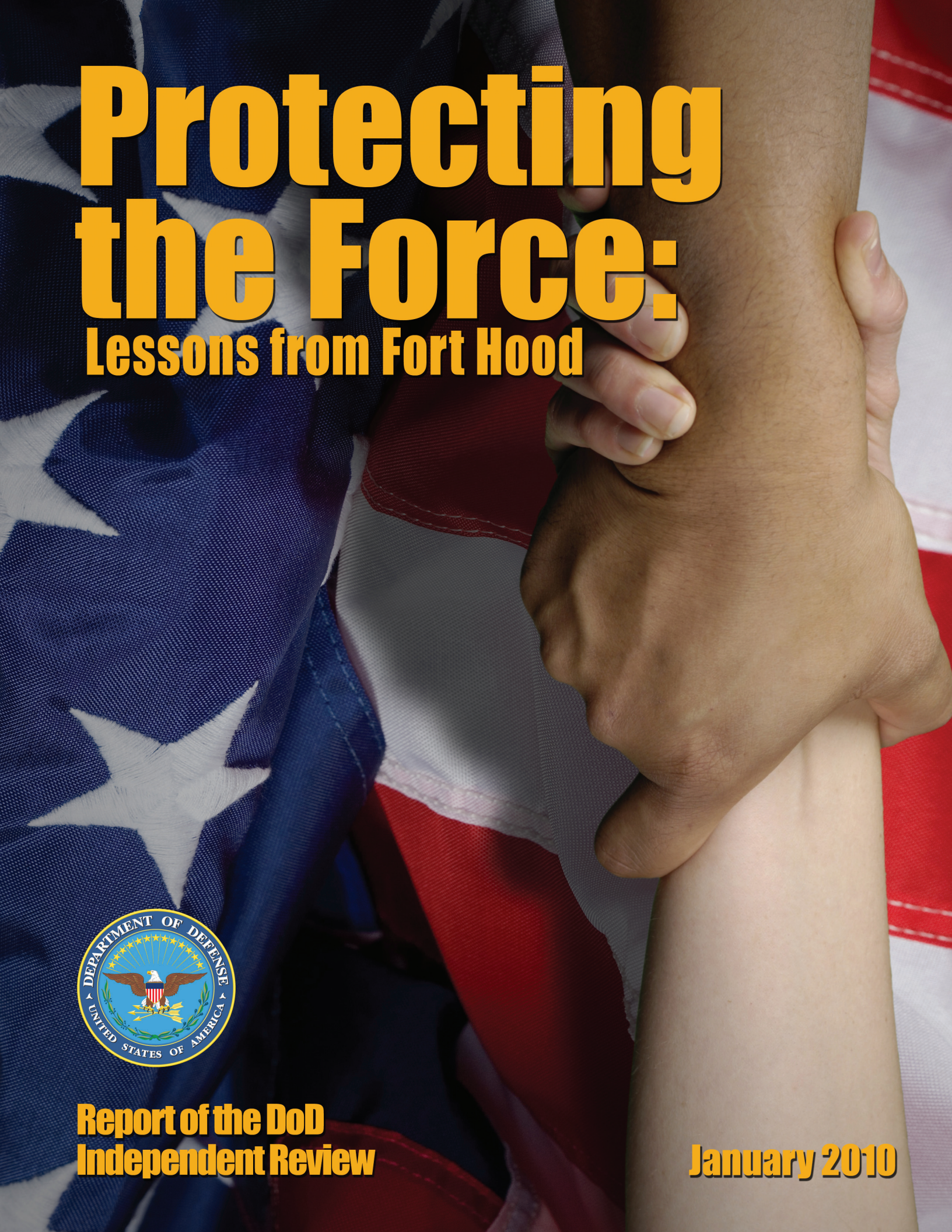


Protecting the Force:

Lessons from Fort Hood

Report of the DoD Independent Review

January 2010

DoD Independent Review Related to Fort Hood

Secretary of Defense

Dr. Robert M. Gates

Co-Chairs

The Honorable Togo Dennis West, Jr.

Admiral Vern Clark, U.S. Navy (Ret).

Board of Advisors

Admiral Kirkland Donald, U.S. Navy

General Stephen Lorenz, U.S. Air Force

General Carter Ham, U.S. Army

Lieutenant General Willie Williams, U.S. Marine Corps

Brigadier General Brian Bishop, U.S. Air Force

Rear Admiral Daniel May, U.S. Coast Guard

Team Leads

General Stephen Lorenz, U.S. Air Force

General Carter Ham, U.S. Army

Lieutenant General Frank Panter, U.S. Marine Corps

Rear Admiral Mark Buzby, U.S. Navy

Rear Admiral Karen Flaherty, U.S. Navy

Ms. Sally Donnelly

Executive Director

Colonel David Krumm, U.S. Air Force

Director of Staff

Lieutenant Colonel Donna Turner, U.S. Air Force

Table of Contents

Executive Summary

Overview

On November 5, 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 initial response to the incident was prompt and effective. Two minutes and forty seconds after the initial 911 call, installation first responders arrived on the scene. One-and-a-half minutes later, the assailant was incapacitated. Two ambulances and an incident command vehicle from the post hospital arrived on the scene two minutes and fifty seconds later.

Leaders at Fort Hood had anticipated mass casualty events in their emergency response plans and exercises. Base personnel were prepared and trained to take appropriate and decisive action to secure the situation. The prompt and courageous acts of Soldiers, first responders, local law enforcement personnel, DoD civilians, and healthcare providers prevented greater losses. As so often happens in our military, lessons already learned have led to a well-developed plan to care for the victims and families involved. The tragedy, however, raised questions about the degree to which the entire Department is prepared for similar incidents in the future—especially multiple, simultaneous incidents.

Following the shooting, Defense Secretary Robert M. Gates established the Department of Defense Independent Review Related to Fort Hood, and asked that we lead the effort.

Secretary Gates directed us to report back to him by January 15, 2010, with recommendations to identify and address possible deficiencies in:

- the Department of Defense's programs, policies, processes, and procedures related to force protection and identifying DoD employees who could potentially pose credible threats to themselves or others;
- the sufficiency of the Department of Defense's 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;
- the 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;
- the adequacy of Army programs, policies, processes, and procedures as applied to the alleged perpetrator.

In response, on November 20, 2009, we formed a panel of five teams to assist in conducting the review. At the same time, we established an advisory board that included senior representatives nominated by each of the Services, the Joint Staff, and the U.S. Coast Guard. A staff of full-time military, civilian, and contractor subject-matter experts conducted separate, but integrated lines of inquiry related to:

- Identification of Internal Personnel Threats
- Force Protection
- Emergency Response and Mass Casualty
- Application of Policies and Procedures
- Support to DoD Healthcare Providers

The review focused on the non-criminal aspects of the tragedy and the teams had unrestricted access to DoD facilities and personnel, including site visits to Fort Hood. The investigative teams conducted a thorough review of the alleged perpetrator's training and military records along with a quality review of

the care he provided to patients during his career. The President directed a review of intelligence matters related to the Fort Hood shooting, the FBI is conducting a review of its procedures, and a criminal investigation is underway. It was critical to maintain the integrity of these investigations. This review therefore, as directed, did not interfere with these activities.

As recognized by the Secretary of Defense in stating that he intends to call upon the military departments to conduct in-depth follow-on reviews based on our results, areas in our report will require further study. By design, we have limited the depth of our report in areas that will be covered in follow-on reviews.

Conducting our review, we have reached a number of conclusions and made corresponding recommendations; they are reflected in the chapters that follow. Several, however, warrant particular attention. We address those now.

Protecting the Force: Lessons from Fort Hood

Events such as the Fort Hood shooting raise questions about how best to defend against threats posed by external influences operating on members of our military community.

Over much of the past two decades our forces have been engaged in continuous combat operations. During this time, Soldiers, Sailors, Airmen, Marines, and DoD civilians have performed admirably through a prolonged series of operational deployments. This operational environment has produced the most experienced combat force in our history, but has also brought extended stressors. The Department of Defense is well-equipped and resourced to defend the nation, its people, and our military installations against external threats. Events such as the Fort Hood shooting, however, raise questions about how best to defend against threats posed by external influences operating on members of our military community. While maintaining effective emergency response and preventive measures to counter external threats, the Department is examining with greater attention how it addresses threats originating from disaffected individuals within the force motivated to violence against the force and the nation—the internal threat. Our review of protecting the force against such threats included, but was not limited to:

- identifying and monitoring potential threats—through gathering, analyzing, and acting on information and intelligence;
- providing time-critical information to the right people—through merging and sharing current indicators;
- employing force protection measures—through maintaining adequate preventive measures to mitigate threats;
- planning for and responding to incidents—through immediate emergency response as well as the long-term care for victims of attacks and their families.

In the years since September 11, 2001, the Department of Defense has devoted significant energy and resources toward improving force protection for our people, their families, and our installations.

Consequently, our facilities are more secure and at reduced risk from a variety of external threats. Now is the time to devote that same commitment toward force protection against the internal threat.

Identifying Threats

There are areas where guidance within the Department of Defense and the Services can be improved. Our review of DoD programs, policies, procedures, and processes revealed several areas that we believe can be corrected to begin to close the gaps for our commanders in the field if adopted expeditiously. Commanders are our key assets to identify and monitor internal threats. Our findings and recommendations emphasize creating clarity for our commanders with respect to identifying behaviors that may pose internal threats and sharing that information within the Department and with other agencies.

DoD force protection policies are not optimized for countering internal threats.... The lack of clarity for comprehensive indicators limits commanders' and supervisors' ability to recognize potential threats.

DoD force protection policies are not optimized for countering internal threats. These policies reflect insufficient knowledge and awareness of the factors required to help identify and address individuals likely to commit violence. This is a key deficiency. The lack of clarity for comprehensive indicators limits commanders' and supervisors' ability to recognize potential threats. Current efforts focus on forms of violence that typically lend themselves to law enforcement intervention (e.g., suicide, domestic violence, gang-related activities) rather than on perceptions of potential security threats. To account for possible emerging internal threats, we encourage the Department to develop comprehensive guidance and awareness programs that include the full range of indicators for potential violence.

Sharing Information

We believe a gap exists in providing information to the right people. The mechanisms for sharing potential indicators of internal threats with appropriate command channels are limited. DoD leaders have continually examined and revised policies regarding inappropriate behavior since the mid-1990s—our force is better as a result of these initiatives. We now find ourselves at a point where we must give commanders the tools they need to protect the force from new challenges.

Since the Fort Hood incident, our leaders have directed changes that improve our information sharing capabilities. We can and should do more. The time has passed when bureaucratic concerns by specific entities over protecting "their" information can be allowed to prevent relevant threat information and indicators from reaching those who need it—the commanders. In this rapidly changing security environment throughout our government, the Department of Defense can exercise its role to set the bar higher to establish a new force protection culture, with new standards and procedures for sharing information, to recognize and defeat evolving external and internal threats.

Force Security

…our commanders must become attuned to behavioral indicators that signal when individuals may commit violent acts or become radicalized.

The current definition for prohibited activities is incomplete and does not provide adequate guidance for commanders and supervisors to act on potential threats to security. Current policies on prohibited activities provide neither the authority nor the tools for commanders and supervisors to intervene when DoD personnel at risk of potential violence make contact or establish relationships with persons or entities that promote self-radicalization. Our commanders need that authority now.

As we seek to understand this new dimension of force protection, our commanders must become attuned to behavioral indicators that signal when individuals may commit violent acts or become radicalized. There is no well-integrated means to gather, evaluate, and disseminate the wide range of behavioral indicators which could help our commanders better anticipate an internal threat. We need to refine our understanding of what these behavioral signals are and how they progress. We encourage the Department of Defense to review, and if necessary expand, the definition of prohibited activities to respond to the rapidly changing security environment.

Who is in Charge?

An effective protection system requires robust information sharing and command and control structures that facilitate active information gathering on potential threats, and disseminating the analysis and assessments of the threat derived from such indicators to the appropriate levels of command. While leaders at Fort Hood responded well under the stress of a rapidly evolving crisis, we are fortunate that we faced only one incident at one location. We cannot assume that this will remain the case in the future.

Our command and control systems must have the right architecture, connectivity, portability, and flexibility to enable commanders to cope with near-simultaneous incidents at multiple locations. Commanders also require the tools to intercept threats before they conduct their attacks, physical barriers, and access controls to prevent unauthorized access, and appropriate response forces to defeat attackers who have gained access to DoD facilities.

Considering the requirements for dealing with multiple, near-simultaneous incidents similar to Fort Hood, a review of the Unified Command Plan may be in order. Gaps in our ability to provide proper command and control and support to subordinate commands should be explored in a variety of ways including conferences, symposia, war games, and exercises.

Reacting to the Event

While major improvements have occurred since September 11, 2001, the Department of Defense must continue to refine its abilities to provide emergency response in concert with other agencies and jurisdictions. In 2009, the Department directed the Services to be in compliance with the Federal framework for emergency response by 2014. Compliance with this guidance will enhance the ability

of the Department's installation and facility emergency personnel to work with first responders from Federal, State, and local jurisdictions to save lives and protect property. We encourage a review to assess the feasibility of accelerating our compliance with the deadline.

Mass casualty events require a rapid transition from normal operations to a surge capability and rapid coordination of services and functions to ensure effective disaster response. The life-saving response to the shooting at Fort Hood was made possible, in part, by strong leadership at all levels. It also depended on existing agreements with local agencies and organizations. The agreements worked, but the command has identified areas for improvement and has set a course to update its memoranda of understanding and otherwise to improve this process. To this end, we recommend improving guidance on tracking, exercising, and inspecting mutual aid agreements. Providing implementing guidance that incorporates the core Service elements and requirements for family assistance in crisis and mass casualty response plans will result in a more resilient force.

The life-saving response to the shooting at Fort Hood was made possible, in part, by strong leadership at all levels.

We especially note that as a result of the Force Protection Condition imposed by Fort Hood leadership during the crisis, a number of young school children remained closeted in their classrooms for a significant period. Our recommendation is that those responsible for them at school (e.g., teachers, administrative personnel) receive additional training to anticipate the special needs that could arise during a period of lengthy lockdown.

We encourage the Department to search for best practices such as those employed at Fort Hood—wherever they originate—to enhance our ability to protect the force.

The Fort Hood response to the shooting was a result of local commanders training their people before the crisis occurred. First responders used active shooter tactics and procedures to stop the attack one-and-a-half minutes after arriving on the scene. These new tactics, originating in civilian law enforcement, focus on neutralizing the threat as quickly as possible. Protecting the force relies on a unified effort to mitigate threats before they materialize, and employing security forces, including those trained to defeat active shooters, in response to attacks on DoD facilities.

We believe there is something positive to be learned from the active shooter training program employed at Fort Hood. Protecting the force against internal threats requires specialized skills and tactics required to respond to active shooter scenarios; while these capabilities may not be appropriate for all DoD law enforcement personnel, we need to develop a range of response capabilities and options. We encourage the Department of Defense to search for best practices such as those employed at Fort Hood—wherever they originate—to enhance our ability to protect the force.

Traumatic events, especially those like the Fort Hood incident that occur in an environment perceived as safe, create new challenges related to supporting and treating individuals directly involved, those in the immediate community, and those in surrounding social networks. Long term behavioral health is the issue. We recommend establishing guidance that includes provisions for both combat and domestic support.

Our examination underscored that the Chaplain Corps has a great deal to offer in a mass casualty situation. Responding to mass casualty events requires more than the traditional first responder disciplines such as police, fire, and medical professionals. Comprehensive religious support that anticipates mass casualty incidents should be incorporated into installation emergency management plans and exercises.

The Department of Defense has a structure to promulgate guidance for Casualty Assistance and Mortuary Affairs Policy. Each program has an oversight board responsible for developing and recommending policy guidance to ensure uniform care of military members and their families and guidance pertaining to new casualty and mortuary entitlements.

Lessons derived from the Fort Hood incident emphasize the importance of current published entitlements in DoD and Service guidance and the need for further guidance regarding new entitlements. Our review highlighted an absence of guidance pertaining to private citizens who become casualties on military installations within the continental United States. The Department of Defense should evaluate policies for casualty reporting, assistance to the survivors, and mortuary services for private citizens who are injured or die on military installations.

How we handle military mental healthcare affects operational readiness.

Our healthcare providers play an important role as force multipliers, keeping our fighting force physically and mentally fit. How we handle military mental healthcare affects operational readiness. We encourage the Department of Defense to evaluate the best programs both inside and outside the Department to inform policies that create a new standard for sustaining healthcare readiness—care for both warriors and providers.

Our care providers are not immune to the cumulative psychological effects of persistent conflict. They serve alongside our combat forces where they experience, share, and help our troops cope with the fears, grief, and concerns that accompany war. Providers, however, often do not avail themselves of access to support resources similar to those that they supply to our fighting forces. Our review suggests that a culture exists in which military healthcare providers are encouraged to deny their own physical, psychological, and social needs to provide the necessary support to beneficiaries. Supporting and sustaining those who care for our forces translates to a healthy workplace, a culture of trust and respect, and healthcare providers who are invigorated rather than depleted by their intimate professional connections with traumatized patients.

The Alleged Perpetrator

As directed in the Terms of Reference, we reviewed the accession, training, education, supervision, and promotion of the alleged perpetrator of the incident at Fort Hood. Through one of our teams, we have devoted a great deal of attention to this issue. As a result of our review, we recommend that the Secretary of the Army review officership standards among military medical officer supervisors at the Uniformed Services University of the Health Sciences and Walter Reed Army Medical Center.

A related issue involves apparent discrepancies between the alleged perpetrator's documented performance in official records and his actual performance during his training, residency, and fellowship.

Some signs were clearly missed; others ignored. That, too, as well as accountability for the discrepancies should be part of a thorough Army review.

Going Forward

We recognize that the events of November 5, 2009, are, first and foremost, a tragedy for all involved: families, colleagues, and the nation. This event shows us, too, that there are no safe havens—for Soldiers, Sailors, Airmen, Marines, their co-workers and their families.

The Department's security posture for tomorrow must be more agile and adaptive.

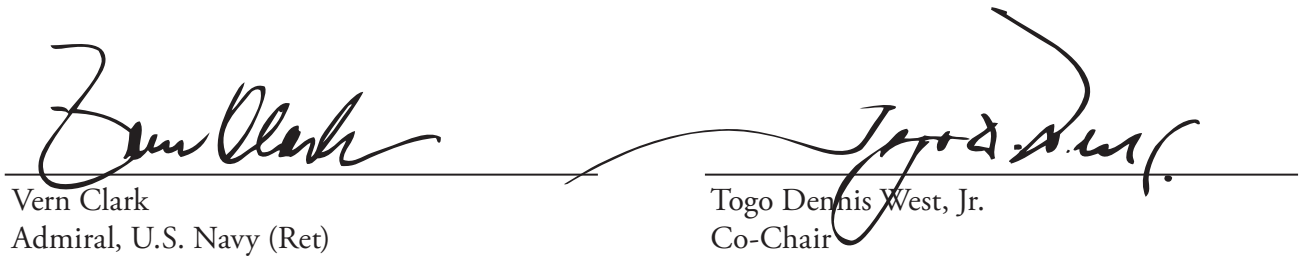
The challenge for the Department of Defense is to prepare more effectively for a constantly changing security environment. The Department's security posture for tomorrow must be more agile and adaptive. This means structures and mechanisms which anticipate the most pressing current threats—like the insider threat today—and the new threats that will manifest themselves in the future.

It has been said that it takes an event to make us consider what is happening to us. In light of events at Fort Hood on November 5, 2009, and of our findings in this report, we believe there are several immediate actions the Secretary of Defense should consider which will enhance our force protection posture.

- Communicate immediately to the force, by direct message from the Secretary, the overriding requirement for commanders, supervisors, non-commissioned leaders, and fellow members of the force to reinforce the fabric of trust with one another by engaging, supervising, mentoring, counseling, and simple everyday expressions of concern on a daily and continuous basis. We must be alert to the mental, emotional, and spiritual balance of Service members, colleagues, and civilian coworkers, and respond when they appear at risk.
- Reinforce the serious effects of failure to reflect fully, accurately, and completely all aspects of professional, ethical, and personal career development in performance appraisals. We can only deal with internal threats if we can rely on the quality of the information reported in our official records.
- Emphasize officership, the embodiment of the military profession that includes leadership, management, and mentoring. Responding to the challenges that now confront us requires a high degree of professionalism from the entire force, but especially from our officers. Our officer corps must instill and preserve the core traits that sustain the profession to keep our forces strong, effective, and safe. Failures in adhering to those standards must be appropriately addressed.
- Synchronize the Continental United States (CONUS)-based DoD emergency management program with the national emergency management framework. Our installations must have a common operating system that allows commanders to access real-time threat information, respond rapidly to changing force protection conditions, and begin response and recovery operations in near real time. This is an aggressive goal, but it matches the goals and character of future enemies.
- Act immediately with the Federal Bureau of Investigation to enhance the operation of the Joint Terrorism Task Forces. To protect the force, our leaders need immediate access to information pertaining to Service members indicating contacts, connections, or relationships with organizations promoting violence. One additional step may be to increase Service representation on the Joint Terrorism Task Forces.

- Create a Secretary of Defense initiative: establish a functional body to concentrate in one place the effort to gather, analyze, and interpret data useful in identifying indicators of potential for violent action; and create a comprehensive and usable catalogue of those indicators with constant updates. The products would be made available to the Department of Defense. Two such possibilities are a Secretary of Defense Initiative on Indicators of Violence, or a Defense Committee on the Recognition of the Indicators of Violence. These would be composed of acknowledged experts drawn from in and outside the Department, such as academia, research institutes, business, former public service, and the like operating under the oversight of an appropriate senior Defense official.

As the Department of Defense considers this review and seeks to improve its force protection posture, our leaders must be mindful that the vast majority of our people are trustworthy and dedicated to defending the nation. How we provide for the security of our installations, our personnel, and their families while simultaneously respecting and honoring their service, is a question that will define force protection, personnel policies, emergency response, and personnel oversight in the years to come.



Vern Clark
Admiral, U.S. Navy (Ret)
Co-Chair

Togo Dennis West, Jr.
Co-Chair

Chapter 1
Oversight of the Alleged Perpetrator

We reviewed pertinent Uniformed Services University of the Health Sciences (USUHS) and Army programs, policies, processes, and procedures as applied to the alleged perpetrator from his accession into USUHS in 1997 to November 4, 2009. This period included his medical training while a student at USUHS from 1997 to 2003, residency at Walter Reed Army Medical Center from 2003 to 2007, a fellowship at Walter Reed Army Medical Center from 2007 to 2009, and assignment at Fort Hood from May 2009 to November 2009.

This part of the review assessed:

- the adequacy and execution of Army programs, policies, processes, and procedures as applied to the alleged perpetrator;
- whether Army and other programs, policies, processes, and procedures functioned properly across the alleged perpetrator's career as a mental health provider to retain and promote him in the Army Medical Corps;
- whether Army programs, policies, processes, and procedures governing separation from the Army of personnel determined not to be fully qualified, or to be unsuitable for, continued military service (without regard to whether the individual is subject to a continuing service obligation), functioned appropriately as applied to the alleged perpetrator;
- whether the care provided by the alleged perpetrator to patients and former patients met accepted standards of care.

We conclude that although the policies we reviewed were generally adequate, several officers failed to comply with those policies when taking actions regarding the alleged perpetrator.

We conclude that although the policies we reviewed were generally adequate, several officers failed to comply with those policies when taking actions regarding the alleged perpetrator. We recommend that you refer matters of accountability for those failures to the Secretary of the Army for appropriate action.

We also recommend that you direct further action on two key concerns identified during our review. We believe that some medical officers failed to apply appropriate judgment and standards of officership with respect to the alleged perpetrator. These individuals failed to demonstrate that officership is the essence of being a member of the military profession, regardless of the officer's specialty. We also found that some medical officers failed to include the alleged perpetrator's overall performance as an officer, rather than solely his academic performance, in his formal performance evaluations. An individual's total performance, academic and non-academic, in a school environment must be a part of the formal performance evaluation process to preclude decisions on that individual's career from being flawed because of incomplete information.

Both types of failures, in our view, were significant and warrant immediate attention.

Our detailed findings, recommendations, and complete supporting discussions, are the restricted annex, some portions of which are not releasable to the public in accordance with applicable law.

Our review also included a quality of care review of the clinical care the alleged perpetrator provided to patients. A memorandum summarizing those results is in the annex. Section 1102 of title 10, United States Code, prohibits the public disclosure of the results of quality of care reviews.

This page intentionally left blank.

Chapter 2
Personnel Policies

We reviewed over 700 documents spanning more than 35,000 pages of DoD and Service directives, instructions, regulations, manuals, command policies, orders, memoranda, and pamphlets, for potential gaps in the Department of Defense's ability to prevent violent acts against military and civilian employees with two objectives:

- Identify and address possible gaps and deficiencies in the programs, policies, processes, and procedures related to identifying DoD military and civilian personnel who could potentially pose credible threats to themselves or others.
- Provide actionable recommendations to improve current programs, policies, processes, and procedures.

We limited the review to military personnel (i.e., Active Duty, National Guard, Reserves), and DoD civilian employees over the lifecycle of DoD employment—from entry to separation. The review did not include Non-Appropriated Fund employees, contractors, retirees, dependents, or policy related to union bargaining agreements. Although we did not address policies concerning contractors, we strongly recommend that they be addressed in a future review.

At the foundation of the Department of Defense's internal security apparatus, we found that there are no significant gaps or deficiencies in programs, policies, processes, and procedures related to the following:

- Personal reliability programs
- Service Member release and discharge policies and procedures
- Medical screening programs to determine initial suitability prior to specialization, and follow-on/ ongoing screening

We separated our Findings and Recommendations into the following categories:

- **Indicators** that DoD personnel may become a danger to themselves or others
- **Reporting and sharing information** about the indicators
- **Barriers or constraints on taking action** or intervention when the indicators are known or recognized by appropriate authority

Indicators that DoD Personnel May Become a Danger to Themselves or Others

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.

Discussion

Research into the causes and predictors of violence spans decades and multiple disciplines (see Appendix D, Literature Review of Risk Factors for Violence). Different disciplines (e.g., psychology, sociology, biology, theology) offer varying perspectives regarding why some people resort to violence. These include genetic and biological causes; specific mental illnesses and personality disorders; reactions to medications or substance abuse; religion, social, and political motivations; and environmental factors. The causes of violence do not fall neatly into discrete categories, and several factors may combine to trigger violent behaviors.

The Department of Defense needs to understand and be prepared for the wide range of motivations and methods, including self-radicalization, distress over relationship problems, association with hate groups, and resentment over perceived personal and professional slights by others within the organization. Research also highlights a range of risk-assessment tools that could enhance our ability to deal with such potential internal threats.

In October 2009, the FBI Behavioral Science Unit established a Military Violence Unit to assist the Department of Defense with coming to grips with this problem. The FBI has spent decades developing methodologies and collecting information to understand the motivations and behaviors of violent offenders. The expertise and perspective derived from law enforcement could be an effective step in helping to identify and mitigate risk factors for DoD personnel.

Recommendation 2.1

- Update training and education programs to help DoD personnel identify contributing factors and behavioral indicators of potentially violent actors.
- Coordinate with the FBI Behavioral Science unit's Military Violence unit to identify behavioral indicators that are specific to DoD personnel.
- Develop a risk assessment tool for commanders, supervisors, and professional support service providers to determine whether and when DoD personnel present risks for various types of violent behavior.
- Develop programs to educate DoD personnel about indicators that signal when individuals may commit violent acts or become radicalized.

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.

Discussion

Background checks on civilians entering the military or DoD civilian workforce have a variety of limitations. State and local laws restrict access to some sealed juvenile records.[1] Some populations (medical, legal, and chaplain officers who receive Direct Commissions into the Reserves[2] and some civilian employees[3]) enter the workforce before the results of their background checks have been received, and a limited number of DoD employees (i.e., temporary civilian workers) are not subject to mandatory background checks at all, although they can be requested.[4]

In the Fort Hood incident, the alleged perpetrator held an active and current SECRET security clearance based on a February 2008 National Agency Check with Local Agency and Credit Check of background investigation. Although accomplished in accordance with current guidelines, this background investigation did not include a subject interview or interviews with co-workers, supervisors, or expanded

1 Title 5 USC, Part III, Subpart H, Chapter 91, Section 9101, *Access to Criminal History Records for National Security and Other Purposes*, Jan. 1, 2005.

2 Department of Defense. DoD 5200.2-R, *Personnel Security Program,* Washington, D.C., Feb. 23, 1996, 33-4.

3 Department of Defense. DoD 5200.2-R, *Personnel Security Program,* Washington, D.C., Feb. 23, 1996, 32.

4 Department of Defense. DoD 5200.2-R, *Personnel Security Program,* Washington, D.C., Feb. 23, 1996, 31.

character references.[5] We believe that if a more thorough investigation had been accomplished, his security clearance may have been revoked and his continued service and pending deployment would have been subject to increased scrutiny.[6]

DoD adjudicative guidelines are vague and training on how and to whom significant information reports are made is insufficient.

DoD adjudicative guidelines are vague and training on how and to whom significant information reports are made is insufficient. They do not provide commanders and their personnel with clear distinctions or thresholds for what constitutes significant information that should be forwarded. Instead, the criteria reflect "whole person" evaluations that are characterized by shades of gray.[7] Our research revealed that limitations on definitions of questionable behaviors result in an aversion to reporting potentially adverse information that does not cross the threshold of criminal activity once a clearance has been granted.[8] The result is a system in which information viewed in isolation may not trigger a review, but the totality of the information viewed in hindsight would clearly indicate a need for such a review.

Due to the critical demand for linguists, interrogators, cultural advisors, etc., for contingency operations, DoD elements have developed expedited processes for citizenship and clearances for DoD personnel. These processes are more limited in scope and could be exploited by adversary groups.

Recommendation 2.2

- Evaluate background check policies and issue appropriate updates.
- Review the appropriateness of the depth and scope of the National Agency Check with Local Agency and Credit Check as minimum background investigation for DoD SECRET clearance.
- Educate commanders, supervisors, and legal advisors on how to detect and act on potentially adverse behaviors that could pose internal threats.
- Review current expedited processes for citizenship and clearances to ensure risk is sufficiently mitigated.

Finding 2.3

DoD standards for denying requests for recognition as an ecclesiastical endorser of chaplains may be inadequate.

5 Telephone Interview with Deputy Director of the Army CAF. Washington, D.C., Dec. 3, 2009.

6 Department of the Army. AR 380-67, *Personnel Security Program,* Washington, D.C., Sep. 9, 1988, 15-16.

7 "National Security Positions." Code of Federal Regulations Title 5, Pt. 732.101-401, 1991 ed., Jan. 4, 2004; Office of the White House Press Secretary. Executive Order 12968, *Access to Classified Information,* Washington, D.C., Aug. 4, 1995; The White House. "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," Washington, D.C., Dec. 29, 2005; Department of the Army. AR 380-67, *Personnel Security Program;* Department of the Navy. SECNAVI 5510.30B, *Personnel Security Program,* Washington, D.C., Oct. 6, 2006; United States Air Force. AFI 31-501, *Personnel Security Program Management,* Washington, D.C., Jan. 27, 2005.

8 Interview with HQ USMC Manager for Information and Personnel Security Program. Washington, D.C., Dec. 16, 2009.

Discussion

Each religious organization that provides military chaplains provides an endorsing agent to serve as its representative to the Department of Defense. These endorsing agents issue and withdraw professional credentials in accordance with the practice of their religious organizations. Current policy requires removal of any individual or religious organization from participation in the DoD Chaplain program only if they threaten national or economic security, are indicted or convicted of an offense related to terrorism, or if they appear on the annual State Department list of Foreign Terror Organizations. This limited authority to deny requests for designation as ecclesiastical endorsers could allow undue improper influence by individuals with a propensity toward violence.

Recommendation 2.3

Review the limitations on denying requests for recognition as ecclesiastical endorsers of chaplains.

Finding 2.4

The Department of Defense has limited ability to investigate Foreign National DoD military and civilian personnel who require access to DoD information systems and facilities in the U.S. and abroad.

Discussion

This further relates to finding, discussion, and recommendation 2.2.

A number of populations presently granted physical access to DoD facilities require some form of vetting for repeated access. Vetting is often a one-time event that does not provide for continuous re-investigation or re-evaluation for the duration of DoD affiliation. For the notionally vetted populations, some records do not exist, and large numbers of people who gain access to our facilities are not vetted at all under current procedures. The Department of Defense's ability to investigate foreign national DoD employees who live outside of the U.S. and require access to DoD facilities is very limited. The Department of Defense is only able to conduct the FBI name check, fingerprint check, and a check of the known and suspected terrorist databases.

Recommendation 2.4

Coordinate with the Department of State and Office of Personnel Management to establish and implement more rigorous standards and procedures for investigating Foreign National DoD personnel.

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.

Discussion

This further relates to finding, discussion, and recommendation 2.1.

DoD and Service policies provide broad pre-deployment guidance on health risk assessment,[9] and

9 Department of Defense. DoDI 6490.03, *Deployment Health,* Washington, D.C., Aug. 11, 2006, 27; Department of Defense. DoDI 6025.19, *Individual Medical Readiness,* Washington, D.C., Jan. 3, 2006, 4.

specific guidance on a variety of high-risk health conditions.[10] Guidance on high-risk health conditionsis useful to healthcare providers currently treating service members. There is no global violence risk assessment performed during pre-deployment for Service members not currently receiving healthcare. Post-deployment assessments, performed at the end of deployment and three to six months after deployment, rely primarily on self-report screening questionnaires[11] to identify risk factors. These screening questionnaires address issues such as post-traumatic stress, traumatic brain injury, substance abuse, depression, and suicide—there are no screening questions to assess the potential to harm others. Moreover, the assessments do not address additional risk factors (i.e., financial, occupational, relationship stressors) thought to be associated with the potential for violence.

Recommendation 2.5

- Assess whether pre- and post-deployment behavioral screening should include a comprehensive violence risk assessment.
- Review the need for additional post-deployment screening to assess long-term behavioral indicators that may point to progressive indicators of violence.
- Revise pre- and post-deployment behavioral screening to include behavioral indicators that a person may commit violent acts or become radicalized.
- 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.

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.

Discussion

This further relates to finding, discussion, and recommendation 2.2.

Suicide Prevention,[12] Sexual Assault Prevention & Response,[13] and Family Advocacy[14] programs address numerous facets of violence. Family Advocacy and Sexual Assault Prevention & Response programs

10 Department of Defense. *ASD Policy Memo on Guidance for Deployment Limiting Psychiatric Conditions & Medications,* Washington, D.C., Nov. 7, 2006, 1-7.

11 Department of Defense. DD Form 2796, *Post Deployment Health Assessment (PHDA),* Washington, D.C., January 2008, 1-7; Department of Defense. DD Form 2900, *Post Deployment Health Assessment (PHDA),* Washington, D.C., January 2008, 1-5.

12 Department of the Air Force. AFI 44-154, *Suicide and Violence Prevention Education and Training,* Washington, D.C., Jan. 3, 2003/Aug. 28, 2006, 2-18; Department of the Army. AR 600-63, *Army Health Promotion,* Washington, D.C., Sep. 20, 2009, 13; Department of the Navy. OPNAVINST 1720.4A, *Suicide Prevention Program,* Washington, D.C., Aug. 4, 2009, 1-10; Department of the Navy. MCO P1700.24B, *Marine Corps Personal Services Manual,* Washington, D.C., Dec. 27, 2001, 3-8.

13 Department of Defense. DoDD 6495.01, *Sexual Assault Prevention and Response Program,* Washington, D.C., Oct. 6, 2005/Nov. 7, 2008, 1-5; Department of the Air Force. AFI 36-6001, *Sexual Assault Prevention and Response Program,* Washington, D.C., Sep. 29, 2009, 5-30; Department of the Navy. SECNAVINST 1752.4A, *Sexual Assault Prevention and Response,* Dec. 1, 2005, 1-5; Department of the Army. AR 600-20, *Army Command Policy,* Washington, D.C., Nov. 30, 2009, 68-82; Department of the Navy. MCO 1752.5, *Sexual Assault Prevention and Response Program, Marine Corps Personal Services Manual,* Washington, D.C., Sep. 28, 2004.

14 Department of the Defense. DoDD 6400.01, *Family Advocacy Program*, Washington, D.C., Aug. 23, 2004, 2-5; Department of the Air Force. AFI 40-301, *Family Advocacy,* Washington, D.C., Nov. 30, 2009, 5-30; Department of the Army. AR 608-18, *Family Advocacy Program,* Washington, D.C., Oct. 30, 2007, 11-71; Department of the Navy. SECNAVINST 1752.3B, *Family Advocacy Program,* Nov. 10, 2005, 1-16; Department of the Navy. MCO P1700.24B, *Marine Corps Personal Services Manual,* Washington, D.C., Dec. 27, 2001, 5-4.

Useful resources for violence prevention education and training also exist in other federal agencies but are dated and not integrated into DoD policies, procedures, or processes.

in each of the Services are implemented based on DoD level guidance, while Suicide Prevention programs are implemented by each of the Services without specific DoD level policy. The policies and procedures at the DoD or Service level that address workplace violence are not comprehensive. Where current policy or programs exist, they are limited, not widely disseminated, and implemented inconsistently.[15] For example, Air Force Instruction 44-154, *Suicide and Violence Prevention Education and Training,* addresses training for both violence and suicide prevention, but the violence prevention portion of annual training was recently eliminated. In recent years, the Services have developed programs that address preventing violence in various populations.[16] These may serve as useful resources for developing more comprehensive workplace violence prevention—including the potential for self-radicalization. Useful resources for violence prevention education and training also exist in other federal agencies but are dated and not integrated into DoD policies, procedures, or processes.[17]

Recommendation 2.6

- Revise current policies and procedures to address preventing violence toward others in the workplace.
- 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.

Finding 2.7

DoD policy regarding religious accommodation lacks the clarity necessary to help commanders distinguish appropriate religious practices from those that might indicate a potential for violence or self-radicalization.

Discussion

DoD Instruction 1300.17, *Accommodation of Religious Practices within the Military Services,* states that requests for religious accommodation should be granted when the practice will not have an adverse impact on mission accomplishment, military readiness, unit cohesion, standards, or discipline.[18] It does not, however, provide standards or recording procedures necessary to establish a baseline of traditional religious practice within faith groups. The Department of Defense has not issued clear guidance on the degree to which the Religious Freedom Restoration Act[19] applies to the military. Therefore, commanders, supervisors, and chaplains lack a common source to distinguish mainstream religious

15 Senior military mental health providers consulted for the DoD Fort Hood Independent Review Panel.

16 Army Warrior Transition Center Policy Memo: Warrior Transition Unit/Community-Based Warrior Transition Unit (WTU/CBWTU) Risk Assessment & Mitigation Policy (Draft pending approval); Department of the Air Force. SG DOC: 06-0009, Memorandum, ALMAJCOM/SG, Washington, D.C., Oct. 14, 2005, 1-9; Combat and Operational Stress First Aid for Caregivers Training Manual (Draft pending approval).

17 Office of Personnel Management. *Dealing with Workplace Violence: A Guide for Agency Planners,* February 1998; Office of Personnel Management. *A Manager's Handbook: Handling Traumatic Events,* Washington, D.C., December 1996.

18 Department of Defense. DoDI 1300.17, *Accommodation of Religious Practices Within the Military Services,* Washington, D.C., Feb. 10, 2009, 2.

19 Title 42, USC Chapter 21B, Religious Freedom Restoration, Section 2000bb-1, *Free Exercise of Religion Protected,* Washington, D.C., Jan. 8, 2008.

practices from extreme practices for faith groups. Service policies and procedures, therefore, vary in stating and reporting standards of religious accommodation.[20]

If requests for religious accommodation that compete with mission requirements were recorded and shared among commanders, supervisors, and chaplains, it would help establish a baseline from which to identify deviations within the Services and the Department of Defense. At present, there is confusion about what is acceptable.

For example, the Air Force requires personnel who request waivers for accommodation of religious apparel to be interviewed by a chaplain to assess whether the request is in keeping with doctrinal or traditional observances of the Service member's faith. Then the installation's senior chaplain must document the findings before forwarding to the commander for a decision. The Services have different procedures for handling religious accommodation requests. None of this information is shared, even when serving together at joint bases or in deployed locations.

This lack of clarity creates the potential for denying information to commanders and supervisors that may signal indicators of self-radicalization or extremist behavior. Commanders and supervisors may not recognize unusual religious practices outside traditional norms within faith groups. Current procedures do not provide consistent mechanisms for initiating appropriate action to prevent an escalation toward violence.

Clear standards would enhance commanders' and supervisors' ability to promote the climate necessary to maintain good order and discipline, and would reduce both the instances and perception of discrimination among those whose religious expressions are less familiar to the command.[21]

Recommendation 2.7

Promptly establish standards and reporting procedures that clarify guidelines for religious accommodation.

Finding 2.8

DoD Instruction 5240.6, *Counterintelligence (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.

Discussion

This relates to finding, discussion, and recommendation 2.1.

DoD Instruction 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs,* provides guidance to conduct defensive counterintelligence and counter-terrorism awareness briefings to DoD personnel. This instruction does not, however, provide specific, updated guidance to the Services, Combatant Commands, and appropriate agencies concerning behavioral indicators that could identify self-radicalization, terrorism, or violence. Researchers and intelligence professionals have been actively

20 Department of the Army. AR 165-1, *Chaplain Activities in the United States Army, Religious Support,* Washington, D.C., Dec. 3, 2009, 1, 9; Department of the Navy. SECNAVINST 1730.8B, *Accommodation of Religious Practices,* Washington, D.C., Oct. 2, 2008, 1-9; Department of the Air Force. AFPD 52-1, *Chaplain Service,* Washington, D.C., Oct. 2, 2006, 2.

21 Department of Defense. DoDI 1300.17, *Accommodation of Religious Practices Within the Military Services,* Washington, D.C., Feb. 10, 2009, 1-2.

engaged in identifying trends in this domain, particularly since September 11, 2001.[22] The absence of an updated and comprehensive policy on emerging threats inhibits the timely update of relevant Service regulations.

Recommendation 2.8

Update DoD Instruction 5240.6 to provide specific guidance to the Services, Combatant Commands, and appropriate agencies for counterintelligence awareness of the full spectrum of threat information, particularly as it applies to behavioral indicators that could identify self-radicalization.

Reporting and Sharing Information About the Indicators

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.

Discussion

This relates to finding, discussion, and recommendation 2.1 and 2.2.

The only information that follows Service members across all assignments is contained in performance evaluations and medical records. Other information may be required, but those requirements vary across the Services.[23] Some information included in these files is temporary, however, and is barred from becoming part of permanent records.[24] For example, Service policies place strong emphasis on commander discretion to record and/or forward information about minor law enforcement or disciplinary infractions.[25] Successful completion of substance abuse counseling is another example of information that may not be included in Service member records, but research studies show that ongoing or past alcohol and drug abuse can lead to violent acts.[26]

The result is that significant additional information is kept at local levels, or for limited periods of time, and is therefore unavailable to future commanders and supervisors. Similarly, incoming commanders and supervisors may lack visibility into some relevant events that occurred prior to their arrival (although some programs such as the Marine Corps' Family Readiness Officer Initiative aim to bridge some of these gaps[27]). Federal law and DoD implementing policies direct certain types of information that

22 Paul K. Davis and Kim Cragin, eds. *Social Science for Counterterrorism.* (2009); Carol Dyer, Ryan E. McCoy, Joel Rodriguez, and Donald N. Van Duyn. "Countering Violent Islamic Extremism." FBI Law Enforcement Bulletin (2007): 3-9; Samuel Nunn. "Incidents of Terrorism in the United States, 1997-2005." *Geographical Review* 97:1 (2007): 89-111; Sánchez-Cuenca, Ignacio and Luis de la Calle. *"Domestic Terrorism: The Hidden Side of Political Violence."* Annual Review of Political Science 12 (2009): 31-49; Smith, Brent. *"A Look at Terrorist Behavior: How They Prepare, Where They Strike."* NIJ Journal 26p0 (2008): 2-6; Austin T. Turk *"Sociology of Terrorism."* Annual Review of Sociology 30 (2004): 271-86.

23 Department of Army. AR 600-37, *Unfavorable Information,* Washington, D.C., Dec. 19, 1986, 3; Department of the Air Force. AFI 36-2608, *Military Personnel Record System,* Washington, D.C., Aug. 30, 2006, 36; Department of the Navy. BUPERSINST 1070.27B, *Document Submission Guidelines for the Electronic Military Personnel Record System,* Washington, D.C., Aug. 26, 2005, 2-4.

24 Department of the Navy. MCO P1070.12K, *Marine Corps Individual Records Administration Manual,* Washington, D.C., July 14, 2000, 1-4, 1-7.

25 Ibid.

26 U.S. Army Center for Health Promotion and Preventive Medicine, Investigation of Homicides at Fort Carson, Colorado, Nov. 2008-May 2009, July 2009, Table B-6, *"Risk Factor Characteristics by Index Case Based on Record Review and Administrative Databases,"* B-14.

27 Department of the Navy. NAVMC Directive 1754.6A, *Marine Corps Family Team Building,* Washington, D.C., Jan. 30, 2006, 2-3 through 2-6; Department of the Navy. MCO 1754.6A, *Marine Corps Family Team Building,* Washington, D.C., Jan. 30, 2006, 4-5, 7.

must and/or cannot be maintained.[28] The Department of Defense's review of guidance for retaining and sharing of additional information should include a recommendation on modifying applicable statutes and policies.

Recommendation 2.9

- 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.
- Develop supporting policies and procedures for commanders and supervisors to access this information.

Finding 2.10

There is no consolidated criminal investigation database available to all DoD law enforcement and criminal investigation organizations.

Discussion

DoD criminal investigation organizations have limited ability to search for or analyze information outside their own databases; they must query other DoD criminal investigation organizations to obtain specific investigative information. This limitation restricts investigative efforts for searches or analysis of data outside of each Service and could reduce the effectiveness of law enforcement to prevent, detect, or investigate criminal activity.

Current initiatives regarding joint basing, coupled with the routine formation of Joint Task Forces, highlight the importance of sharing investigative data among the Services.

Current initiatives regarding joint basing, coupled with the routine formation of Joint Task Forces, highlight the importance of sharing investigative data among the Services. The Department of Defense has recognized this shortfall and supported implementation of a Defense Law Enforcement Exchange, using the Naval Criminal Investigative Service's Law Enforcement Information Exchange (LInX) as a model. LInX is a database established to apply search and link analysis tools by providing access to structured and unstructured data across organizations, including Federal, State, county, and municipal agencies.

Recommendation 2.10

Establish a consolidated criminal investigation and law enforcement database such as the Defense Law Enforcement Exchange.

Finding 2.11

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.

28 36 Code of Federal Regulation, Part 1220, *Federal Records - General,* Washington, D.C., Nov. 2, 2009; 36 Code of Federal Regulation, Part 1222, *Creation and Management of Federal Records,* Washington, D.C., Nov. 2, 2009; Department of Defense. DoDD 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials,* Washington, D.C., Jan. 15, 1986/ Dec. 20, 1989, 3.

Discussion

This relates to finding, discussion, and recommendation 2.10.

DoD policy requires the Secretaries of the Military Departments and Directors of the Defense Agencies to establish local contact points in subordinate commands for coordination with Federal, State, and local civilian law enforcement officials.[29] The Services have implemented this directive through various Service-specific documents, ranging from mandatory guidance in seeking formal Memoranda of Understanding to encouraging partnerships with local law enforcement agencies. The latitude in seeking agreements with Federal, State, and local law enforcement could, however, create gaps in the Services' ability to identify DoD personnel who might pose a credible threat to themselves or others. Without strong liaison agreements, commanders and supervisors lack visibility of a Service member's criminal acts committed off a military installation. This could impede the ability of a commander or supervisor to assess indicators that signal when individuals may be prone to committing violent acts or falling prey to self-radicalization.

The Services include provisions in their respective antiterrorism guidance regarding DoD requirements to implement effective processes to integrate and fuse all sources of available threat information from local, State, Federal, and host nation law enforcement agencies.[30] An exclusive focus on antiterrorism, however, fails to consider an escalation of violent criminal behavior. The absence of effective information sharing agreements creates a potentially critical void in a commander's ability to assess his personnel.

Recommendation 2.11

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, with clearly established standards regarding scope and timeliness.

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.

Discussion

Release of protected health information in the Department of Defense is governed by the Health Information Portability and Accountability Act (HIPAA), which balances confidentiality with the need to ensure operational readiness and is reflected in DoD and Service-level policy.[31] Unique guidance on release of medical information has been established for Restricted Reporting in cases of sexual assault.[32]

29 Department of Defense. DoDD 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials,* Washington, D.C., Jan. 15, 1986/Dec. 20, 1989, 3.

30 Department of Defense. DoDI 2000.16, *DoD Antiterrorism (AT) Standards,* Washington, D.C., Oct. 2, 2006/Dec. 8, 2006, 14.

31 Department of Defense. DoDI 6025.18-R, *Privacy of Individually Identifiable Health Information in DoD Health Care Programs,* Washington, D.C., Jan. 24, 2003, 19, 25, 49; Department of Defense. DoDI 6490.4, *Requirements for Mental Health Evaluations of Members of the Armed Forces,* Washington, D.C., Aug. 28, 1997, 7-8, 11-13, 14-15; Department of Defense. DoDD 36490.1, *Mental Health Evaluations of Members of the Armed Forces,* Washington, D.C. , Oct. 1, 1997, 5-7; Department of the Air Force. AFI 44-109, *Mental Health Confidentiality and Military Law,* Washington, D.C., Mar. 1, 2000, 2, 3, 9; Department of the Army. MEDCOM Policy 09-027, *Release of Protected Health Information to Unit Command Officials,* Washington, D.C., May 19, 2009, 1-5.

32 Department of Defense. DoDD 6495.01, *Sexual Assault Prevention and Response Program,* Washington, D.C., Oct. 6, 2005/Nov. 7, 2008, 3-4.

The Department of Defense has recently provided interim guidance that indicates the circumstances under which it is appropriate and required for a healthcare provider to release protected health information.[33] Not all current Service-level guidance reflects the most recent DoD policy.

Recommendation 2.12

Ensure Services update policies to reflect current DoD-level guidance on the release of protected health information.

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.

Discussion

This relates to finding, discussion, and recommendation 2.1.

Civilian health professionals who provide care to Service members have several sets of guidelines that govern response to indicators of violence that are determined during treatment. Policy does not require civilian providers to notify military health treatment facilities or commanders, and in some cases—especially when the information involves personal data—it prohibits information transfer to anyone except authorized family members. This gap in visibility prevents military medical providers, commanders, and supervisors from assisting the Service member or intervening until the risk indicators result in observable behaviors that trigger concern.

Recommendation 2.13

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.

Finding 2.14

The Department of Defense does not have a comprehensive and coordinated policy for counterintelligence activities in cyberspace. There are numerous DoD and interagency organizations and offices involved in defense cyber activities.

Discussion

This relates to finding, discussion, and recommendation 2.1.

The evolving security threat increasingly involves information exchanges using the Internet. The Services have developed cyber counterintelligence programs to identify potential threats to DoD personnel, information, and facilities. Non-DoD agencies are also involved in cyber counterintelligence activities. The Department of Defense does not have an overarching policy coordinated across the interagency and with the Office of the Director of National Intelligence that provides clear guidance to the Services and

33 Department of Defense. DTM 09-006, *Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel,* Washington, D.C., July 2, 2009, 1-6.

Defense agencies on the execution of counterintelligence cyber activities. The Department of Defense is reviewing comments from the Services and appropriate defense agencies on Draft DoD Instruction 5240.mm, *Counterintelligence Activities in Cyberspace.*

Recommendation 2.14

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

Barriers or Constraints on Taking Action

Finding 2.15

DoD policy governing prohibited activities is unclear and does not provide commanders and supervisors the guidance and authority to act on potential threats to good order and discipline.

Discussion

This relates to finding, discussion, and recommendation 2.1.

DoD policy on prohibited activities is limited and only addresses active participation in groups that may pose threats to good order and discipline.

DoD policy on prohibited activities is limited and only addresses active participation in groups that may pose threats to good order and discipline.[34] However, this does not include contacting, establishing, and/or maintaining relationships with persons or entities that interfere with or prevent the orderly accomplishment of the mission or present a clear danger to loyalty, discipline, mission, or morale of the troops.[35] All of these activities may increase an individual's propensity to commit violence, and should be within the purview of commanders to address.

Recommendation 2.15

Review prohibited activities and recommend necessary policy changes.

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.

Discussion

This relates to finding, discussion, and recommendation 2.1.

The Department of Defense's authorities for civilian personnel are more limited than for military members. For a variety of reasons, many indicators of risk factors associated with violence are not visible to commanders and supervisors, especially factors that might be observed outside the workplace. Even

34 Department of Defense. DoDI 1325.06, *Handling Dissident and Protest Activities Among Members of the Armed Forces,* Nov. 27, 2009, 9.

35 The Supreme Court has recognized differing freedom of speech and freedom of association standards for military members and civilians. For a comparative discussion, see U.S. v. Brown, 45 M.J. 389, at 395 (CAAF, 1996).

within the workplace, not all civilians are subject to some of the screening procedures that might reveal indicators of concern.

The ability to address some civilian behaviors that may be associated with violence is limited by DoD and Service policies, statutes, federal regulation, and collective bargaining agreements.

The ability to address some civilian behaviors that may be associated with violence is limited by DoD and Service policies, statutes, federal regulation, and collective bargaining agreements. As one example, Air Force regulations specify that supervisors seeking to suspend a civilian employee from the workplace must provide at least 24-hour notice to that employee, and the policies note that seven-day notice is more typical.[36] This authority is likely insufficient if an employee represents an imminent threat.

Recommendation 2.16

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.

36 Department of Defense. DTM 09-006, *Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel,* Washington, D.C., July 2, 2009, 1-6; Department of Air Force. AFI 36-704, *Discipline and Adverse Actions,* Washington, D.C., July 22, 1994, 13.

This page intentionally left blank.

Chapter 3
Force Protection

An impenetrable shield against all threats remains neither practical nor affordable. However, a force protection system that encompasses a variety of tactics, techniques procedures, and technology to deter and, if necessary, defeat an attack against our people has proven effective.

Our study found that some policies governing information exchange, both within the Department of Defense and between the Department and outside agencies, are deficient and do not support detection and mitigation of internal threats. There is not a well-integrated means to gather, evaluate, and disseminate the wide range of behavioral indicators that could signal an insider threat.

We addressed key supporting pillars such as physical security, installation access, indications and warning, and information sharing.

We reviewed DoD, Joint, Service, and Northern Command and its Service Components force protection policies and implementing guidance to determine consistency across the Department of Defense, identify potential best practices that could be shared/adopted, determine if there were contradictions in force protection policies, and identify deficiencies that, if corrected and implemented, could prevent another Fort Hood occurrence within the Department of Defense. In addition to DoD personnel, we contacted Department of Homeland Security and FBI officials to gather information, confirm policies, or to seek best practices.

Authorities/Command and Control

Finding 3.1

- The Department of Defense has not issued an integrating force protection policy.
- Senior DoD officials have issued DoD policy in several force protection-related subject areas such as antiterrorism, but these policies are not well integrated.

Discussion

Joint Publication 3-0 defines force protection as preventive measures taken to mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information.[37]

Multiple senior DoD officials have responsibility for various force protection-related programs: Under Secretary of Defense for Personnel and Readiness for several law enforcement personnel and health affairs policies; Under Secretary of Defense for Policy for antiterrorism, terrorism suspicious activity reporting, continuity of operations, and critical infrastructure protection policies; Under Secretary of Defense for Acquisition, Technology, and Logistics for installation emergency management; and Under Secretary of Defense for Intelligence for physical security, military working dog, counterintelligence, use of deadly force, and carrying of firearms for law enforcement and security duties policies. No senior DoD official is assigned overall responsibility for force protection policy and there is no integrating DoD policy regarding force protection.

No senior DoD official is assigned overall responsibility for force protection policy and there is no integrating DoD policy regarding force protection.

37 Department of Defense. Joint Publications 3-0, *Joint Operations,* Washington, D.C., Sep. 17, 2009.

The President has assigned the mission of force protection to the Geographic Combatant Commanders in the Unified Command Plan. Only one of the DoD force protection-related policies (Antiterrorism) addresses this mission. In DoD Directive 2000.12, *DoD Antiterrorism Program,* the Deputy Secretary of Defense assigned the Geographic Combatant Commanders tactical control for force protection for most DoD personnel in their geographic areas of responsibility.[38] No other DoD policy addresses this mission.

Our review suggests that there is some misunderstanding regarding the scope of the geographic combatant commanders' force protection responsibility and the responsibility of the military departments, especially in the United States. If multiple, simultaneous events similar to the Fort Hood incident occur, clarity of command and control responsibilities will be essential for a rapid, comprehensive response.

Recommendation 3.1

- Assign a senior DoD official responsibility for integrating force protection policy throughout the Department.
- Clarify geographic combatant commander and military department responsibilities for force protection.
- Review force protection command and control relationships to ensure they are clear.

Indications and Warning

Finding 3.2

DoD force protection programs and policies are not focused on internal threats.

Discussion

This relates to finding, discussion, and recommendation 2.1.

Detecting and defeating an internal threat requires close personal observation and interaction rather than the construction of physical security barriers. Current DoD and Service programs that provide guidance concerning observation of personal behavior are primarily medically oriented and focused on suicide prevention. There is no formal policy guidance for commanders to identify, report, or act on indicators that may be indicative of an internal threat. There is no DoD-wide protocol to notify commanders of potential internal threats that may exist in their command. Inability to reliably detect and counter emerging internal threats is a gap in DoD force protection measures.

The effort to identify threats posed by those who have access to DoD installations or systems and knowledge of our defensive measures and weaknesses is targeted toward defending specific resources. Whether internal threats target a computer system, classified information, or personnel, research suggests they may often share common indicators.[39] The effort to identify threats may be enhanced by exploiting any common indicators and integrating the disparate programs designed to defend against these threats.

The Services have already cautioned their people to be alert to threats such as terrorism, school violence, sexual crimes, stalking, cyber crimes, domestic violence, arson, sabotage, communicated threats, and

38 Department of Defense. *Unified Command Plan (UCP),* Washington, D.C., Dec. 17, 2008; Department of Defense. DoDD 2000.12, *DoD Antiterrorism (AT) Program,* Washington, D.C., Aug. 18, 2003.

39 Defense Personnel Security Research Center. *Technical Report 09-02: Insider Risk Evaluation and Audit,* Monterey, CA, August 2009.

The Department of Defense does not have a comprehensive training program focused on internal threats regardless of the target.

pre-attack behaviors. Several DoD programs exist (e.g., Counterintelligence Awareness Training, Information Assurance Training, U.S. Army Ten Key Indicators of Terrorist Activity, Suicide Prevention, Personnel Reliability Program) that task members to report suspicious behavior indicative of future destructive acts.[40] These programs and associated training focus on protecting specific assets. The Department of Defense does not have a comprehensive training program focused on internal threats regardless of the target. In addition, the integration and fusion process for command, medical, law enforcement, and chaplain services is not firmly or universally established. For example, an installation's Threat Working Group could be specifically tasked to consider and evaluate internal threats as part of their normal procedure. If individuals of concern are brought to their attention, they could then evaluate and advise the commander on ways to mitigate the potential threat.

Countering the internal threat should focus on the common indicators leading up to a wide range of destructive events, such as terrorism, school violence, sexual crimes, stalking, cyber crimes (cyber stalking), domestic violence, arson, sabotage, communicated threats, and pre-attack behavior. This approach would focus on exhibited behavior regardless of the individual's identity. New programs to address internal threats should take a comprehensive approach and be presented as a means to take care of fellow DoD members from a force protection perspective.

Training programs put in place to educate DoD personnel should be easily understandable by the entire population. Identifying the key indicators of aberrant behavior and clearly outlining the process to report will be critical to focusing the force on the threat. Establishing the process and providing the tools for commanders to evaluate and counter internal threats will be important as well. Predictive analysis for internal threats is a difficult proposition, but predicting and defending against external threats requires a similar degree of anticipation.

The Navy has a fusion cell designed to predict and mitigate insider violence that could serve as a model for the Department of Defense. The Naval Criminal Investigative Service established the Threat Management Unit in 1996.[41] The Threat Management Unit provides criminal and behavioral analysis and risk assessments for Navy and Marine Corps commanders to predict and mitigate potential violence on the part of DoD affiliated personnel. Other examples of successful threat assessment and intervention exist and are worthy of further study. The U.S. Postal Service has a successful workplace violence program highlighted by the use of threat assessment teams.[42] The Association of Threat Assessment Professionals provides additional resources integrating academic, private, and public studies and programs for countering an insider threat.[43]

40 Department of Defense. DoDI 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs,* Washington, D.C., Aug. 7, 2004, 1-16; Department of Defense. DoDD 8570.01, *Information Assurance Training, Certification, and Workforce Management,* Washington, D.C., Aug. 15, 2004, 1-10; Department of the Army. Appendix A ALARACT 322, *Ten Key Indicators of Potential Terrorist Associated Insider Threats to the Army,* Washington, D.C., Nov. 23, 2009; Department of the Army. *Army Campaign Plan for Health Promotion, Risk Reduction and Suicide Prevention (ACPHP),* Washington, D.C., Apr. 16, 2009; Department of Defense. DoD 5210.42-R, *Nuclear Weapons Personnel Reliability Program (PRP) Regulation,* Washington, D.C., Nov. 10, 2009, 1-72.

41 Department of the Navy. *Naval Criminal Investigative Service Operating Manual 3, Manual for Criminal Investigations,* Chapter 29 (Assault), Paragraph 2.6, Threat Management Unit, Washington, D.C., August 2008.

42 United States Postal Service. Washington, D.C., May 1997.

43 The Association of Threat Assessment Professional. *The Association of Threat Assessment Professional (ATAP),* http://www.atapworldwide.org/.

Recommendation 3.2

- Develop policy and procedures to integrate the currently disparate efforts to defend DoD resources and people against internal threats.
- 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 relating to pending violence.
- Provide commanders with a multidisciplinary capability, based on best practices such as the Navy's Threat Management Unit, the Postal Service's "Going Postal Program," and Stanford University's workplace violence program, focused on predicting and preventing insider attacks.

Information Sharing

Finding 3.3

The Department of Defense's commitment to support JTTFs is inadequate.

Discussion

This relates to finding, discussion, and recommendation 2.10.

Defense Criminal Investigative Service involvement at the JTTFs is not functionally managed by the Defense Counterintelligence and Human Intelligence Center, as is the case for the Service linked participants (i.e., Army Military Intelligence, Naval Criminal Investigative Service, Air Force Office of Special Investigations). As a result, there is no consistency of reporting from those agents back to the Department of Defense.[44] The lack of a single functional management structure increases the likelihood of confusion on the part of the FBI when it deals with DoD representatives who operate under different functional guidance. Any outcome should consider Defense Criminal Investigative Service independence and objectivity.[45]

Recommendation 3.3

- Identify a single point of contact for functional management of the Department of Defense's commitment to the JTTF program.
- 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.
- Review the commitment of resources to the JTTFs and align the commitment based on priorities and requirements.

Finding 3.4

There is no formal guidance standardizing how to share Force Protection threat information across the Services or the Combatant Commands.

---

44 Interview with Deputy Director (DCIS) and Homeland Security/Terrorism Program Manager (DCIS). Washington, D.C., Dec. 10, 2009.

45 Department of Defense. DoDD 5106.01, *Inspector General of the Department of Defense,* Washington, D.C., Apr. 13, 2006.

Discussion

This relates to finding, discussion, and recommendation 2.10.

Policy exists stating the requirement to share threat information with the Combatant Commands.[46] When a military criminal investigative organization or a counterintelligence organization outside the construct of a JTTF obtains threat information pertaining to a CONUS asset or individual, there is no standard means to share that information with the Geographic Combatant Commands.

The FBI's draft guidance for informing the Department of Defense of terrorism matters with a DoD nexus, does not cover who, beyond the headquarters of Service Counterintelligence organizations (Army G2X, Air Force Office of Special Investigations, Naval Criminal Investigative Service, and the Defense Counterintelligence and Human Intelligence Center), should be informed of the matter. It is incumbent on those Headquarters elements to comply with requirements to inform the affected appropriate operational commanders or other organizations with a need to know.

Recommendation 3.4

Direct the development of standard guidance regarding how military criminal investigative organizations and counterintelligence organizations will inform the operational chain of command.

Finding 3.5

The Department of Defense does not have direct access to a force protection threat reporting system for suspicious incident activity reports.

Discussion

This relates to finding, discussion, and recommendation 2.10.

Suspicious Activity Reporting or Force Protection Threat Information, as it is known to Department of Defense, is now an FBI nationwide initiative. The Department of Defense was using the Threat and Location Observation Notice Program as its Suspicious Activity Reporting capability, but the program was terminated in September 2007. This left the Department of Defense without a Suspicious Activity Reporting system of its own.[47]

The Deputy Secretary of Defense instructed DoD Components to submit Suspicious Incident/Activity Reports and other non-intelligence reporting concerning force protection threats to the FBI's classified Guardian Reporting System on an interim basis. DoD and FBI guidance for Guardian reporting assures that privacy and civil liberties are protected.[48] This reporting continues today.

The FBI has created an unclassified version of its Guardian system—called eGuardian—providing participating partners with a suspicious activity reporting system.

---

46 Department of Defense. DoDI 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense Agencies,* Washington, D.C., May 14, 2004; Federal Bureau of Investigation. Joint Terrorism Task Force, *Standard Memorandum of Understanding Between the Federal Bureau of Investigation and Defense Criminal Investigation Service,* Washington, D.C., Aug. 31, 2007; Department of Defense. DoDI 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs,* Washington, D.C., Aug. 7, 2004.

47 Interview with Principal Analyst, OASD, Homeland Defense and America's Security Affairs. Washington, D.C., Dec. 16, 2009.

48 Department of Defense. Deputy Secretary of Defense Memorandum, *Implementation of Interim Threat Reporting Procedures,* Washington, D.C., Sep. 13, 2007.

eGuardian is a secure web-based system for sharing potential terrorist threats, terrorist events, and suspicious activity information among Federal, State, local, and tribal law enforcement partners, along with State fusion centers and JTTFs. eGuardian is the only Suspicious Activity Reporting system that communicates directly with the FBI's JTTFs, and if adopted by the Department of Defense would allow designated DoD law enforcement assets access to receive and input suspicious activity. This would also provide an additional method by which threat information would flow from the Department of Defense to the FBI, in situations where the Department of Justice has an investigative interest. Adoption of eGuardian is currently the recommended solution being proposed by the Office of the Assistant Secretary of Defense for Homeland Defense for the Department of Defense.

eGuardian does not replace coordination and information sharing requirements per the 1979 Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with The Federal Bureau of Investigation and the 2009 Memorandum of Understanding between the FBI and the Department of Defense Governing the JTTF relationship.

Recommendation 3.5

- Adopt a common force protection threat reporting system for documenting, storing, and exchanging threat information related to DoD personnel, facilities, and forces in transit.
- Appoint a single Executive Agent to implement, manage, and oversee this force protection threat reporting system.

Finding 3.6

There are no force protection processes or procedures to share real-time event information among commands, installations, and components.

Discussion

This relates to finding, discussion, and recommendation 2.10.

During the initial stages of the attack at Fort Hood, commanders and first responders, unsure of the nature of the threat, and in an effort to maximize their security posture, set and maintained Force Protection Condition Delta. There were apparently no indications that the rest of CONUS DoD force was immediately notified of the event; most installations and units first found out about the event through the news media. This was a single event, but had it been the first in a series of coordinated, near simultaneous attacks, most other DoD installations and facilities would not have been properly postured for an attack. The timely sharing of incident information could have served to alert other forces within the Area of Responsibility to take the prepare-and-defend actions necessary to harden themselves before a near simultaneous attack comes to them.

The requirement for a process/system to share raw, non-validated event information in near real time is the key ability for alerting the force that an attack is underway. The present DoD reporting and alerting system, a system based on phone calls and Defense Messaging System message traffic, is neither timely nor able to share information simultaneously among all user levels—from tactical users to operational and strategic decision makers.

Recommendation 3.6

Evaluate the requirement for creating systems, processes, policy, and tools to share near real-time, unclassified force protection information among military installations in CONUS to increase situational awareness and security response.

Access Control

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.

Discussion

DoD policy mandates 100 percent credentials inspection for access to DoD CONUS installations.[49] The DoD Physical Security Program Instruction designates the Common Access Card (CAC) as "the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces."[50] While the CAC is the principal identity document, other approved documents may be used by dependents and other DoD affiliated individuals to obtain access. Installations outside CONUS may recognize other identity documents depending on status of forces agreement specifications. In all cases, however, properly credentialed individuals will be granted access to the installation.

Fort Hood is equipped with a state-of-the-art automated access control system, augmented by hands-on inspection of identity credentials that meet or exceed all DoD and Department of the Army guidance. In the case of the Fort Hood incident, the alleged perpetrator was authorized access and was a registered user of Phantom Express, the post's automated access control system. The alleged perpetrator's status as an active duty officer with a CAC meant that he was authorized access to virtually all military installations.

Detecting a trusted insider's intention to commit a violent act requires observation of behavioral cues/ anomalies.

Detecting a trusted insider's intention to commit a violent act requires observation of behavioral cues/anomalies. There are Federal programs that train personnel to observe individuals under routine conditions. Authorities may engage the individual in casual conversation and observe their responses and behavior. When anomalies are detected, the individual is selected for secondary screening, which provides a greater opportunity to detect potential threatening activity. These programs may be useful if employed in a similar manner by DoD security guards, police officers, supervisory personnel, persons working in visitor control centers, or in other common "customer service" contexts.

49 Department of Defense. DoDI 5200.08P, *Security of DoD Installation and Resources,* Washington, D.C., Dec. 17, 2008; Department of Defense. DTM 09-012, *Interim Policy Guidance for DoD Physical Access Control,* Washington, D.C., Dec. 2, 2009; Department of Homeland Security. HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* Washington, D.C., Aug. 27, 2004; National Institute of Standards and Technology. FIPS PUB 201-1, *Federal Information Processing Standards Publication, Personal Identity Verification (PIV) of Federal Employees and Contractors,* Gaithersburg, MD, March 2006.

50 Department of Defense. DoD 5200.08-R, *Physical Security Program: Security of DoD Installation and Resources,* Washington, D.C., May 27, 2009.

Recommendation 3.7

- Review best practices, including programs outside the U.S. Government, to determine whether elements of those programs could be adopted to augment access control protocols to detect persons who pose a threat.
- Review leading edge tools and technologies that augment physical inspection for protecting the force.

Finding 3.8

The Department of Defense does not have a policy governing privately owned weapons.

Discussion

In the absence of overarching DoD policy, the individual Services have established privately owned weapons policies. Service regulations direct that all personnel living in installation housing and those residing in common living areas (barracks) register privately owned weapons with the installation security office. Personnel residing in common living areas must store weapons in unit armories, and those weapons (and ammunition) will be inventoried at specified intervals. Those personnel residing in private on-base family housing may store their weapons in quarters. Service regulations for registering or storing privately owned weapons do not apply when living off installation.

The Services task installation commanders with establishing privately owned weapons regulations on their installations. The Services have established minimum standards, leaving it to commanders to meet installation-specific requirements, including additional guidance on transporting privately owned weapons. Our review conducted a representative sampling of installation policies that revealed prohibitions on transporting loaded firearms and transporting a firearm in the glove compartment of a vehicle. The guidance we reviewed also requires keeping the weapon and ammunition separate while in transit.[51]

Recommendation 3.8

Review the need for DoD privately owned weapons policy.

Finding 3.9

Services cannot share information on personnel and vehicles registered on installations, installation debarment lists, and other relevant information required to screen personnel and vehicles, and grant access.

Discussion

This relates to finding, discussion, and recommendation 2.10.

Services, with Defense Agency support, continue to research and field advanced automated entry control systems designed to expedite authorized entry onto installations. However, these automated

51 Headquarters XVIII Airborne Corps & Fort Bragg. XVIII Airborne Corps & Fort Bragg Regulation 190-12, *Military Police: Privately Owned Weapons and Ammunition Control and Prohibited Weapons,* Fort Bragg, NC, Dec. 1, 2004; Department of Defense. Combat Center Order P1630.6E, *Discipline and Law Enforcement Regulations,* Washington, D.C., Mar. 12, 1997; Department of the Navy. SUBASENLONINST 5500.1C, *Privately Owned Weapons on Naval Submarine Base New London,* Groton, CT, May 18, 2005; Department of the Air Force. AFI31-101 AAFBSUP, *The Air Force Installation Security Program,* Washington, D.C., Apr. 17, 2008; Department of the Navy. MCO 5530.14A, *Marine Corps Physical Security Program Manual,* Washington, D.C., June 5, 2009.

systems do not allow the Services to share information on registered users and persons debarred from one installation to another. The lack of a central authoritative database means that individuals debarred by a command from entering one installation for misconduct, unsuitability, or other reasons may be authorized access to another DoD installation.

Overseas installations do not have access to the National Crime Information Center or the Terrorist Screening Database. Access control systems in CONUS and overseas should be able to authenticate personnel against authoritative databases.

Recommendation 3.9

- Develop timely information sharing capabilities among components including vehicle registration, installation debarment lists, and other access control information.

- Accelerate efforts to automate access control that will authenticate various identification media (e.g., passports, CAC, drivers' licenses, license plates) against authoritative databases.
- Obtain sufficient access to appropriate threat databases and disseminate information to local commanders to enable screening at CONUS and overseas installation access control points.

This page intentionally left blank.

Chapter 4

Emergency Response and Mass Casualty

The Department of Defense must synchronize and align its emergency management program with national response guidance. Using common emergency management principles, we can prepare our military communities to respond to emergencies—from the smallest incident to the largest catastrophe. Our nation uses a framework and system to guide the response to any hazard.[52] These provide a consistent template enabling all jurisdictions and organizations across the country to prepare for, respond to, and recover from emergencies using a unified response. Synchronizing the Department of Defense's emergency management program with this national guidance will ensure the Department can integrate effectively with all partners in response to any and all emergencies.

Emergency Response

Finding 4.1

Services are not fully interoperable with all military and civilian emergency management stakeholders.

Discussion

The Department of Defense guidance was promulgated in part to align the Department with national response policies and establish the Installation Emergency Management program.[53] The Installation Emergency Management program directs the Services to adopt the National Incident Management System, which Federal, State, and local agencies have already adopted. The Department of Defense has given the Services until January 13, 2011, to develop their initial capability, and until January 13, 2014, to have a full Installation Emergency Management program aligned with national guidance. The instruction directing the Services to comply with the national system directed the Services to develop their own implementation plans and timelines.[54] Currently all 50 states have complied with the Federal requirements. There are, however, no measures or established milestones in DoD guidance to define initial and full capability.

The Department of Defense will experience challenges in reaching full capability in the absence of centralized policy because of synchronization and funding issues. Technical capabilities such as 911/dispatch, mass notification, information sharing, and Common Operating Picture could delay full capability because of the cost of some systems.

The Installation Emergency Management program identifies how first responders from on and off the installation integrate into a unified effort during emergency response and recovery operations. This Installation Emergency Management plan is designed to become the installation's umbrella plan, which nests functional area plans, thus enhancing coordination between responders.

Until full operational capability is achieved, integration between installation and facility emergency personnel and other first responders will continue to be largely based on personal relationships rather than on codified procedures.

52 Department of Homeland Security. *National Response Framework,* Washington, D.C., Jan. 2008, 1-12. Department of Homeland Security. *National Incident Management System,* Washington, D.C., December 2008, 45-62.

53 Department of Defense. DoDI 6055.17, *DoD Installation Emergency Management Program,* Washington, D.C., Jan. 13, 2009, 2.

54 Ibid.

Current Air Force guidance[55] puts the Air Force ahead of schedule for achieving full compliance with the Installation Emergency Management program. Reviews of the Air Force approach suggest possible best practices for consideration by other Services.

Recommendation 4.1

- Establish milestones for reaching full compliance with the Installation Emergency Management program.
- Assess the potential for accelerating the timeline for compliance with the Installation Emergency Management program.

Implementation of Enhanced 911

Finding 4.2

There is no DoD policy implementing public law for a 911 capability on DoD installations.[56] Failure to implement policy will deny the military community the same level of emergency response as those communities off base.

Discussion

Rapid communications, particularly major communication nodes such as 911 Dispatch Centers, are critical in an emergency response. Congress mandated Enhanced 911 services as the national standard but it has not been fully implemented by the Department of Defense.[57]

Our review identified the following deficiencies:

- 911 is not the universal emergency assistance number on DoD installations
- Not all installations have enhanced 911 capability
- Some installations have 911 calls going on and off the installation to different dispatch centers depending upon what type of phone is used (e.g., cell phones, Defense Switching Network phones)

While no major 911 delays were identified in the Fort Hood After Action Review (AAR),[58] 911 calls from cell phones and family housing were routed through the Bell County Emergency Dispatch Center, which had to relay the information verbally to the Fort Hood Dispatch center. Fort Hood then dispatched first responders to the incident. Calls from on base[59] telephones went directly to the Fort Hood Dispatch Center. Since Fort Hood does not have Enhanced 911 capability, the caller's location and information was not available. Had callers from cell phones and family housing wanted to reach the Fort Hood Dispatch Center directly, they would have had to use a phone number other than 911.

55 Department of the Air Force. AFI 10-2501, *Air Force Emergency Management Program Planning and Operations,* Washington, D.C., Apr. 6, 2009; Department of the Air Force. AF Manual 10-2504, *Air Force Incident Management for Major Accidents and Disasters,* Washington, D.C., Dec. 1, 2009; Department of the Air Force. AF Manual 10-2502, *Air Force Incident Management System Standards and Procedures,* Washington, D.C., Sep. 25, 2009.

56 Public Law. 106-81, *Wireless Communications and Public Safety Act of 1999,* Washington, D.C., Oct. 26, 1999; Public Law. 108-494, *Enhance 911 Services.* Washington, D.C., Dec. 23, 2004.

57 Public Law. 108-494, *Enhance 911 Services,* Washington, D.C., Dec. 23, 2004, Section 102 Findings, Section 102; The law incorporates state-of-the-art telecommunications capabilities to 911 systems.

58 HQ III Corps and Fort Hood. *Fort Hood After Action Review,* Fort Hood, TX, November 5, 2009, Slide 22.

59 For the purpose of this report we consider "on base" to mean calls made on Defense Switching Network (DSN). Calls from DSN go directly to the Fort Hood Department Emergency Services Dispatch.

By having the Department of Defense implement Enhanced 911 services policy, dispatch centers would have access to vital information about a caller's location and identification in case the call is lost, or if the caller becomes incapacitated. This capability would also help reduce response times and increase coordination among all responders. Failure to implement policy will deny the military community the same level of emergency response as those communities off base.

Recommendation 4.2

Develop policy that provides implementation guidance for Enhanced 911 services in accordance with applicable laws.[60]

Law Enforcement Practices–Active Shooter Threat

Finding 4.3

DoD policy does not currently take advantage of successful models for active shooter response for civilian and military law enforcement on DoD installations and facilities.

Discussion

This review identified tactics, techniques, and procedures that exist within the civilian community to respond to the active shooter scenario. An active shooter is generally described as an individual(s) actively engaged in killing people in a confined and populated area. Typically there is no pattern or method to their selection of victims.[61] Unfortunately, no DoD policy exists for active shooter scenarios, and the Department of Defense has no established process to quickly adopt civilian law enforcement best practices.

Despite the absence of DoD guidance, the Services have included the active shooter protocol in their civilian police training.

Current active shooter response protocols came out of the Columbine tragedy, which transformed police procedures and tactics for dealing with shooting rampages. Prior to Columbine the tactic was to isolate and call in a special response team.[62] After Columbine, police departments collectively developed new active shooter response protocols with the goal being to neutralize the threat immediately. The Fort Hood AAR[63] noted that the installation's Department of Emergency Services began training this new active shooter response protocol last year and during this incident the responding officers attributed their actions to this new training protocol.[64]

60 Public Law. 106-81, *Wireless Communications and Public Safety Act of 1999,* Washington, D.C., Oct. 26, 1999; Public Law. 108-494, *Enhance 911 Services,* Washington, D.C., Dec. 23, 2004.

61 Department of Homeland Security. *Active Shooter: How to Respond,* Washington, D.C., 2008, 7.

62 Marine Corps Police Academy. Lesson Plan 9.2, *Active Shooter,* October 2008, 8; Marine Corps Police Academy. Study Guide 9.2, *Active Shooter,* October 2008, 5.

63 HQ III Corps and Fort Hood. *Fort Hood After Action Review,* Fort Hood, TX, Nov. 5, 2009, Slide 23.

64 Police Officer Sgt. Kimberly Munley was trained through Advanced Law Enforcement Rapid Response Training (A.L.E.R.R.T.) which equips first responders with tactical skills and training on how to stop active shooters; Davis, Bianca. *First Responder: Officer who ended massacre trained by Texas State program,* Nov. 10, 2009. http://star.txstate.edu/content/first-responder-officer-who-ended-massacre-trained-texas-state-program, (accessed Dec. 10, 2009).

The Secretary of the Army is the Executive Agent charged with developing minimum training standards for civilian police and security guard training.[65] However, the current minimum standards do not include active shooter response protocols. Despite the absence of DoD guidance, the Services have included the active shooter protocol in their civilian police training.[66] It is not, however, included in the training for military law enforcement members.

The Air Force has included guidance on this particular topic in AFI 31-201, *Security Forces Standards and Procedures.*[67] In this instruction, the response to an active shooter threat is specifically addressed as a command responsibility, and requires that active shooter protocols be incorporated into installation plans. This is by far the most comprehensive direction in published Service policies, and could be considered a best practice.

While the Fort Hood AAR does not address the actions of the victims and other bystanders during the assault this is an area that requires examination. Typically, individuals involved in these situations have never considered how to react under these circumstances, including how to react when law enforcement officers arrive on the scene. There are a variety of training tools available that address employee responses during workplace violence situations. The Department of Homeland Security publishes a pamphlet which provides basic training and awareness of appropriate actions people can and should take during this type of threat.[68] The Department of Defense has no equivalent training tool. It could, however, be incorporated into an existing personal security training program such as that found in the Level 1 Antiterrorism Awareness annual training requirement.[69]

Recommendation 4.3

- Identify and incorporate civilian law enforcement best practices, to include response to the active shooter threat, into training certifications for civilian police and security guards.
- Include military law enforcement in the development of minimum training standards to ensure standard law enforcement practices throughout the Department of Defense.
- 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.[70]
- Develop a case study based on the Fort Hood incident to be used in installation commander development and on-scene commander response programs.

---

65 Department of Defense. DoDI 5210.90, *Minimum Training, Certification, and Physical Fitness Standards for Civilian Police and Security Guards in the Department of Defense,* Washington, D.C., July 9, 2007; Department of Defense. Deputy Assistant Secretary of Defense Memorandum, *Designation of the Secretary of the Army as the DoD Executive Agent for Training, Certification, and Physical Fitness Standards for DoD Civilian Police Officers and Security Guards,* Washington, D.C., Jan. 4, 2006.

66 In some instances it is identified in specific tactics, techniques, and procedures, such as the Navy's Law Enforcement And Physical Security For Navy Installations publication; Department of the Navy. NTTP 3-07.2.3, *Law Enforcement and Physical Security for Navy Installations,* Washington, D.C., June 2009, 5-4 – 5-7.

67 Department of the Air Force. AFI 31-201, *Security Forces Standards and Procedures,* Washington, D.C., Mar. 30, 2009, 31; High Risk situations in Chapter 9 states "Security Forces must take immediate action to neutralize the threat." Further, it requires that "Installation plans…must address the use of Security Forces to isolate, contain, and neutralize a terrorist, active shooter, or hostage incident, with or without assistance."

68 Department of Homeland Security. *Active Shooter: How to Respond,* Washington, D.C., 2008, 1-20.

69 Department of Defense. DoDI 2000.16, *DoD Antiterrorism Standards,* Washington, D.C., Oct. 2, 2006.

70 Ibid.

Mass Warning and Notification

Finding 4.4

Based on Joint Staff Integrated Vulnerability Assessments, many DoD installations lack mass notification capabilities.

Discussion

DoD Instruction 6055.17 on Installation Emergency Management directs all installation commanders to "develop mass warning and notification capabilities with the ability to warn all personnel within 10 minutes of incident notification at the dispatch center."[71] *DoD Antiterrorism Standards* also require that mass notification systems be incorporated into emergency response planning.[72] The specific standards, requirements, and applications for all mass notification systems are contained in the Unified Facilities Criteria.[73]

At Fort Hood the emergency operations center effectively used their "Big Voice" system as part of their response protocol during the incident. As mentioned in the AAR:

> *Soldiers were notified through loud speaker to return to their units for accountability and to advise the Post of the situation and to issue instructions. Use of the Big Voice prevented a lot of phone calls into the Emergency Operations Center for basic information.*[74]

Big Voice (Giant Voice) has been the standard for mass notification on DoD installations. Today, a more comprehensive approach to mass warning using newer technologies is available, such as the Navy's Wide Area Alert and Notification System. It includes Automatic Telephone Notification System and Computer Desktop Notification System capabilities.[75] These capabilities could be coupled with other personal computing devices such as PDAs, text messaging to cell phones, and social networking sites such as Twitter and Facebook. These new technologies have been put to use at numerous universities since the Virginia Tech mass shooting.[76]

Recommendation 4.4

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.

Common Operational Picture

Finding 4.5

Services have not widely deployed or integrated a Common Operational Picture capability into installation Emergency Operations Centers per DoD direction.[77]

---

72 Department of Defense. DoDI 6055.17, *DoD Installation Emergency Management Program,* Washington, D.C., Jan. 13, 2009, 32.

72 Department of Defense. DoDI 2000.16, *DoD Antiterrorism Standards,* Washington, D.C., Oct. 2, 2006, 24.

73 Unified Facilities Criteria 4-021-01, *Design and O&M: Mass Notification Systems,* Dec. 18, 2002.

74 HQ III Corps and Fort Hood. *Fort Hood After Action Review,* Fort Hood, TX, Nov. 5, 2009, Slide 49.

75 Department of the Navy. Draft CNIC Instruction 2000.XX, *CNIC Wide Area Alert Network,* Unpublishd, Paragraph 5.0, System Operational Requirements.

76 Robin Hattersly Gray. *Virginia Tech 1 Year Later: How Campuses Have Responded,* March/April 2008, http://www.campussafetymagazine.com/Articles/?ArticleID=157, (accessed Dec. 8, 2009).

77 Department of Defense. DoDI 6055.17, *DoD Installation Emergency Management Program,* Washington, D.C., Jan. 13, 2009, 31, 39.

Discussion

Information sharing and establishing a Common Operational Picture is vital to coordinating efforts of multiple emergency response agencies' and facilitates' collaborative planning at all echelons to achieve situational awareness. A Common Operational Picture is "a single identical display of relevant information shared by more than one command."[78] A Common Operational Picture provides a standardized, continuously updated, multiple-user capability to produce reports, mapping, imagery, and real time information sharing between multiple subscribers.

DoD guidance directs installations to have a well-defined communication plan with personnel engaged in emergency response, as well as with local first responders. This plan includes a Common Operational Picture and information management system to execute and support actions listed in the Installation Emergency Management Plan and to ensure interoperable communications with civil authorities.

While the Fort Hood AAR is correct in stating that "information sharing and establishing a Common Operational Picture is best conducted at Ops Center,"[79] installation personnel experienced challenges as they attempted to integrate multiple Emergency Operations Centers and establish a Common Operational Picture. At Fort Hood multiple reports of gun shots caused commanders to delay the release of children from the local day care center for six hours due to the lack of situational awareness and communication with on-post organizations.[80]

As the Services deploy this capability, there are current technologies that have been adopted by emergency management organizations across the country such as WebEOC and E-Team. Services need to integrate their Common Operational Picture with technologies used by local community.

Recommendation 4.5

- Examine the feasibility of accelerating the deployment of a state-of-the-art Common Operational Picture to support Installation Emergency Operations Centers.
- Develop an operational approach that raises the Force Protection Condition 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.

Synchronization of Emergency Management Policies and Programs

Finding 4.6

- Stakeholders in the DoD Installation Emergency Management program, including the Under Secretary of Defense for Policy; Under Secretary for Personnel and Readiness; Under Secretary of Defense for Intelligence; Under Secretary of Defense for Acquisition, Technology & Logistics; Assistant Secretary of Defense for Public Affairs; and Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer, have not yet synchronized their applicable programs, policies, processes, and procedures.

79 Department of Defense. Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms,* October 2009, 105.

79 HQ III Corps and Fort Hood. *Fort Hood After Action Review,* Fort Hood, TX, Nov. 5, 2009, Slides 46, 48, 51.

80 HQ III Corps and Fort Hood. *Fort Hood After Action Review,* Fort Hood, TX, Nov. 5, 2009, Slides 11, 65, 70, 74.

- Better synchronization and coordination would remove redundant planning requirements, identify seams in policy, focus programmed resources, and streamline procedures to achieve unity of effort in installation emergency management.

Discussion

The Under Secretary of Defense for Acquisition, Technology & Logistics coordinates DoD programs, policies, processes, and procedures. Several policy documents require installations to develop emergency response and recovery plans related to mass casualty incidents (i.e., disaster plans, antiterrorism plans, emergency response Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) plans, mass disaster, or mass casualty response plans). These stove-piped requirements are embedded within Installation Emergency Management functional area policies such as: fire, antiterrorism, CBRNE, medical, religious support, and casualty affairs.[81] If DoD guidance was better synchronized, these redundant planning requirements could be identified and consolidated. A good example of synchronizing Emergency Management guidance is the Assistant Secretary of Defense for Health Affairs policy for Public Health Emergency Management[82] which requires installation medical treatment facility emergency plans to be integrated with the installation emergency management plan. Better coordination of policy and procedures in this way would lead to the Installation Emergency Management plan becoming the umbrella plan for emergency response and recovery, nesting within it functional area plans in a synchronized manner.

Recommendation 4.6

- Review responsibilities for synchronizing Office of the Secretary of Defense programs, policies, and procedures related to installation emergency management.
- Establish policy requiring internal synchronizing of installation programs, plans, and response for emergency management.

Mutual Aid Agreement

CONUS military installations and their surrounding civilian communities are increasingly interdependent.

Finding 4.7

Mutual Aid Agreements (MAAs) between DoD and civilian support agencies across the Services are not current.

Discussion

CONUS military installations and their surrounding civilian communities are increasingly interdependent. When an emergency or a disaster strikes, it is critical for both parties to rely on established relationships for mutual support. Coordination is normally formalized in mutual aid agreements to meet response requirements following a disaster.

81 Department of Defense. DoDI 6055.06, *DoD Fire and Emergency Services Program,* Washington, D.C., Dec. 21, 2006, 22; Department of Defense. DoDI 2000.16, *DoD Antiterrorism Standards,* Washington, D.C., Oct. 2, 2006, 17; Department of Defense. DoDI 2000.18, *DoD Installation CBRNE Response Guidelines,* Washington, D.C., Dec. 4, 2002, 14; Department of Defense. DoDI 1300.18, *DoD Personnel Casualty Matters, Policies and Procedures,* Washington, D.C., Jan. 8, 2008, 8; Department of Defense. DoDI 6055.17, *DoD Installation Emergency Management Program,* Washington, D.C., Jan. 13, 2009.

82 Department of Defense. Draft DoDI 6200.03, *Public Health Emergency Management Within the Department of Defense,* Washington, D.C., Unpublished, 23; This policy requires a Medical Emergency Manager be appointed as each installation medical treatment facility to serve as the primary point of contact with the Installation Emergency Manager and ensure medical treatment facility emergency management plans are integrated and compliant with Installation Emergency Management program.

Within the medical function area, Department of Defense guidance[83] requires military treatment facilities to meet or exceed the accreditation standards of The Joint Commission (TJC)[84] and to comply with all related management programs.

Ample policy exists across the Department of Defense and Service levels regarding the need to develop and maintain MAAs.[85] Historically those agreements have not been maintained or exercised sufficiently. Functional areas, including fire, engineering, medical, and religious support have relied on MAAs to resolve resource gaps and share capabilities for daily operations and emergencies. To comply with TJC's accreditation standards, hospitals must incorporate robust emergency management planning and coordination. The 12 TJC Emergency Management standards, including 111 Elements of Performance require Medical Emergency Management Planning, coordination, and exercising with local agencies including installation as well as civilian stakeholders. In addition, DoD guidance requires all tenants to participate in Installation Emergency Management planning and all-hazards exercises.[86]

Existing DoD and Service emergency management-related guidance recognizes the need for interagency coordination of agreements to resolve resource gaps that are identified during planning or real world events. Our review, however, found no overarching guidance regarding the maintenance, frequency of review, and tracking of MAAs. The exceptions are guidance for agreements to have legal review[87] and to be signed by a responsible official.[88]

The Fort Hood experience highlighted that MAAs were in place, and were helpful in meeting the emergency response requirements. They had not, however, been tracked and were not exercised sufficiently to ensure currency and effectiveness. This resulted in delays in the installation obtaining information on patients taken to civilian hospitals.[89] Although liaison officers were deployed to assist in obtaining patient information, prior coordination and planning might have facilitated the free flow of information between the civilian hospitals and the installation. As mentioned in our earlier discussion of information sharing, restrictions on what constitutes releasable information under HIPAA and other guidelines further complicate matters in an emergency response scenario. Also, if the agreements had been included in exercises extending past immediate response into consequence management, the shortcoming in information sharing may have been identified.

The Fort Hood incident highlights the value of exercising and practicing response plans with local entities. Maintaining current MAAs and involving civilian hospitals in disaster plan response exercises could enhance the availability of information concerning military patients through military treatment

83 Department of Defense. DoDD 6025.13, *Medical Quality Assurance in the Military Health System,* Washington, D.C., May 4, 2004.

84 As of Jan. 1, 2007 the JCAHO changed its name to The Joint Commission. The Joint Commission. *A Journey Through the History of The Joint Commission.* http://www.jointcommission.org/aboutus/joint_commission_history.htm, (accessed Dec. 9, 2009).

85 Department of the Army. AR 525-27, *Army Emergency Management Program,* Washington, D.C., Dec. 4, 2008, 5; Department of the Navy. BUMED Instruction 3440.10, *Navy Medicine Force Health Protection Emergency Management Program,* Washington, D.C., Nov. 20, 2008, encl. 1, 26; Department of Defense. DoDI 6055.17, *DoD Installation Emergency Management Program,* Washington, D.C., Jan. 13, 2009; Department of Defense. DoDI 2000.18, *DoD Installation CBRNE Response Guidelines,* Washington, D.C., Dec. 4, 2002; Department of the Navy. OPNAV Instruction 3440.17, *Navy Installation Emergency Management Program,* Washington, D.C., July 22, 2005, 4; Department of the Air Force. AF Manual 32-4004, *Emergency Response Operations,* Washington, D.C., Dec. 1, 1995, 22; Department of the Navy. Draft MCO 3440.9, *Marine Corps Installation Emergency Management Program,* Washington, D.C., Unpublished, 3, 7; Department of the Air Force. AFI 32-2001, *Fire Emergency Services Program,* Washington,

86 Department of Defense. DoDI 6055.17, Installation Emergency Management Program Washington, D.C., Jan. 13, 2009.

87 Department of Defense. DoDI 2000.18, *DoD Installation CBRNE Response Guidelines,* Washington, D.C., Dec. 4, 2002; Department of the Army. AR 600-20, *Army Command Policy,* Washington, D.C., Mar. 18, 2008.

88 Department of Defense. DoDI 2000.18, *DoD Installation CBRNE Response Guidelines,* Washington, D.C., Dec. 4, 2002.

89 HQ III Corps and Fort Hood. *Fort Hood After Action Review,* Fort Hood, TX, Nov. 5, 2009, Slides 35, 38.

The Fort Hood incident highlights the importance of extending exercises beyond the immediate response to consequence management to include local agencies.

facilities to commanders. Currently, most exercises are not resourced to extend the scenario beyond hospital emergency departments, leaving gaps in inter-hospital administration process coordination. The Fort Hood incident highlights the importance of extending exercises beyond the immediate response to consequence management to include local agencies.

Recommendation 4.7

Review Installation Emergency Management programs to ensure correct guidance on integrating tracking, exercising, and inspections of MAAs.

Emergency Family Assistance

Finding 4.8

The Department of Defense 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.

Discussion

Following the September 11, 2001, attacks, the Department of Defense established a joint military Services Pentagon Family Assistance Center. The Pentagon Family Assistance Center AAR cited a lack of DoD policy guidance for victim and family support services plans.[90] These plans, as part of the overall emergency response, would have improved communication and coordination and reduced the response time to organize operations during the aftermath of September 11. The Pentagon AAR identified a requirement for synchronizing and coordinating the following 13 functional areas: administration, casualty and mortuary assistance, child care, command and control, communications and information technology, community outreach (i.e., medical, mental health, chaplain), donations management, legal assistance, logistics and operational support, public affairs, resource management, security, and staff and volunteer management.[91]

Our review of DoD publications revealed that the lessons from the terrorist attacks in 2001 resulted in sufficient policy guidance for implementing day-to-day family support programs and baseline family support services. However, this guidance has not been updated nor does it clearly delineate a specific structure for how these services come together and integrate in support of a crisis or mass casualty incident.[92]

The Services have policies that guide family assistance and support services.[93] A review of these policies noted they do not consistently differentiate between services offered routinely and those required in

90 Department of Defense. *Pentagon Family Assistance Center After Action Report,* Washington, D.C., March 2003.

91 Ibid.

92 Department of Defense. DoDD 1342.17, *Family Policy,* Washington, D.C., Nov. 21, 2003, 1-6; Department of Defense. DoDI 1342.22, *Family Centers,* Washington, D.C., Dec. 30, 1992, 7-8.

93 Department of the Army. AR 608-1, *Army Community Services Center,* Washington, D.C., Sept. 19, 2007, Chapter 4-1, 9, Chapter 4-2, 9-10, Chapter 4-4, 10; Department of the Navy. OPNAV Instruction 1754.1B, *Fleet and Family Support Center Program,* Washington, D.C., Nov. 5, 2007, 8; Department of the Navy. MCO P1700.24B, *Marine Corps Personal Services Manual,* Washington, D.C., Dec. 27, 2001, 2-3; Department of the Air Force. AFI 36-3009, *Airman and Family Readiness Centers,* Washington, D.C., Jan. 18, 2008, 1-17.

response to a crisis or mass casualty incident. The exception is the Air Force which incorporated the Pentagon AAR recommendations into its policy. This policy and the companion "Tool Kit" specify unique mission responsibilities and resourcing requirements needed to integrate victim and family services in response to the full spectrum of crises or catastrophic events.[94]

The Services did not consistently implement the guidance from the Pentagon AAR recommendations. The Fort Hood AAR again identified the need for planning for emergency family assistance.[95] This AAR cited instances related to family service and support functions that would have been improved with prior planning, to include donation management, family reception, escort functions, chaplain support, and casualty assistance.[96] As part of the installation's response to the tragic events in November, leaders developed the Fort Hood Behavioral Health Campaign Plan that offers a framework for providing physical, emotional, and spiritual care to those affected by a mass casualty or disaster event.[97] The three core elements identified in the Campaign Plan are among the 13 identified in the Pentagon AAR.

Recommendation 4.8

- Develop guidance incorporating the core service elements of a Family Assistance Center as identified in the Pentagon AAR.
- Develop implementation guidance to establish requirements for a Family Assistance Center crisis and mass casualty response as integral components of Installation Emergency Management plans.
- Consider the Air Force's Emergency Family Assistance Control Center and the Fort Hood Behavioral Health Campaign Plan as possible best practices when developing policy.

Religious Support Integration

Finding 4.9

The lack of published guidance for religious support in mass casualty incidents hampers integration of religious support to installation emergency management plans.

Discussion

Our review of DoD guidance found no instructions that address religious support planning and integration requirements in response to a mass casualty incident. This results in inconsistencies in Service policies on integrating religious support into emergency management, and could lead to inadequate planning and coordination for religious support resources.

Service policies regarding religious support differs among the Services. In the Navy and Marine Corps, the integration of religious support in a mass casualty incident is a base and installation decision. The Marine Corps has a publication that provides crisis ministry guidance.[98] Other than the Army Medical

94 Airman and Family Readiness Center. *Emergency Family Assistance Control Center Tool Kit,* May 2007.

95 HQ III Corps and Fort Hood. *Fort Hood After Action Review,* Fort Hood, TX, Nov. 5, 2009, Slides 81-89.

96 *Fort Hood After Action Review;* Presentation at Fort Hood, TX, Dec. 8, 2009, Slides 81-89.

97 HQ III Corps and Fort Hood. *Fort Hood Behavioral Health Campaign 09-11-665,* Fort Hood, TX, Dec. 7, 2009.

98 U.S. Marine Corps. MCRP 6-12A, *Religious Ministry Team Handbook,* Quantico, VA, May 16, 2003, 5-1, 5-9.

Command's regional Special Medical Augmentation Response Teams,[99] which includes religious support specialists who provide religious support during mass casualty and crisis incidents, there is no overarching Army guidance. Lastly, Air Force instructions[100] designate the chaplain as a formal member of the installation emergency management planning team, the Critical Incident Stress Management Team, the Disaster Response Force,[101] and the Disaster Response Team.[102] The Air Force guidance may be a best practice for consideration in developing DoD policy.

Inconsistencies in DoD policy and Service guidance were illustrated during the Fort Hood incident. When the incident began, the Installation Chaplain was not contacted immediately.[103] As a result, there was a delay in the Chaplain's response to the immediate needs of victims and responders.

Recommendation 4.9

- 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.
- Develop policy for religious support in response to mass casualty incidents and integrate guidance with the Installation Emergency Management Program.

Finding 4.10

Inconsistencies among Service entry level chaplain training programs can result in inadequate preparation of new chaplains to provide religious support during a mass casualty incident.

Discussion

The Services train chaplains in emergency and mass casualty response. However, they provide this training at different times.

The Navy's Chaplain Basic Course provides no formal training in religious support to mass casualty incidents, but upon arrival at their first Navy or Marine Corps duty station, Navy chaplains receive formal instruction in accordance with base or ship emergency management plans.

Air Force chaplains receive mass casualty familiarization training at their Basic Course and then receive more detailed mass casualty training and participate in Major Accident Response Exercises upon arriving at their first duty station.

The Army Chaplain Basic Course includes comprehensive training for religious support during mass casualty incidents. This instructional program is a possible best practice for other Services to consider.

---

99 A current Army manual provides for pastoral care to the sick or wounded; speaks to religious support in the context of Defense Support to Civilian (DSCA) authority; establishes UMTs as members of interdisciplinary case management teams and hospital committees; and expresses what UMTs do in the MASCAL and trauma response realm; Department of the Army. FM 1-05, *Religious Support,* Washington, D.C., Apr. 18, 2003, 2-10.

100 Department of the Air Force. AFI 34-1101, *Assistance of Survivors of Persons Killed in Air Force Aviation Mishaps and Other Incidents*, Washington, D.C., Oct. 1, 2001, 20; *Air Force Emergency Management Program Planning and Operations,* 128-129, 145.

101 Department of the Air Force. AFI 34-1101, *Assistance of Survivors of Persons Killed in Air Force Aviation Mishaps and Other Incidents,* Washington, D.C., Oct. 1, 2001, 20.

102 Department of the Air Force. AFI 52-104, *Chaplain Services Readiness,* Washington, D.C., Apr. 26, 2006, 74-75.

103 Installation Chaplain's presentation at Fort Hood, TX, Dec. 8, 2009.

The Army also conducts an Emergency Medical Ministry Course that is open to Religious Support Teams from all Services to enhance counseling and care skills for traumatic situations.[104]

The Fort Hood Installation Chaplain noted that three new chaplains performed exceptionally well during the November 5, 2009, mass casualty, and he credited their success to the training they received at the Chaplain Basic Course.[105]

Recommendation 4.10

Review mass casualty incident response training in the Chaplain Basic Officer Courses.

Memorial Service Support

Finding 4.11

The Department of Defense 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.

Discussion

Congress established a new entitlement that authorizes travel and transportation to specific family members to attend a memorial service in honor of a deceased service member.[106] To implement these new entitlements DoD guidance is necessary to ensure that they are consistently applied across the Services. Commanders must understand which family members are entitled to funded travel, the time allowed for travel, and any restrictions that may apply. In joint basing, consistent application will be significant when considering the likelihood that members of different Services could become fatalities in the same event.

The Fort Hood incident highlighted the need for this policy. In an effort to support the families of the fallen, the Army requested travel entitlements based on the recent Congressional authorization. Since implementing guidance had not been published, the Army obtained DoD authorization for government funded travel for eligible family members to attend the Fort Hood Memorial Ceremony.

Recommendation 4.11

Develop standardized policy guidance on memorial service entitlements.

104 The Emergency Medical Ministry Course is a two-week, intensive course suitable for all Service Religious Support Teams.

105 Presentation at Fort Hood, TX, Dec. 8, 2009.

106 National Defense Authorization Act for FY 2010. Public Law 111-84, Section 631, *Travel and Transportation for Survivors of Deceased Members of the Uniformed Services to Attend Memorial Services,* Washington, D.C., Oct. 30, 2009.

Private Citizens with No DoD Affiliation

Finding 4.12

- DoD casualty affairs policy,[107] Federal law,[108] and DoD mortuary affairs guidance[109] 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.

Discussion

At Fort Hood, one of the fatalities was a DoD contract employee. Upon review, it became apparent that the death of a private citizen in these circumstances would have presented a situation without clear guidance as to notification policy and the provision of casualty assistance. This review expanded this incident to include all private citizens who frequent military installations.

Our review of DoD and service casualty policies revealed no guidance, at any level, that was sufficient to address the full range of issues pertaining to private citizens who become casualties on a CONUS military installation.[110] In the area of DoD and Service mortuary affairs policies, this review revealed a similar absence of guidance regarding mortuary entitlements and services.[111]

Recommendation 4.12

- 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.
- Review current mortuary affairs policies relating to mortuary services for private citizens who become fatalities on a military installation within CONUS.

107 Department of Defense. DoDD 1300.18, *Department of Defense (DoD) Personnel Casualty Matters, Policies, and Procedures,* Aug. 14, 2009, 1-62.

108 Federal Law. Title 5, United States Code, Section 5742, *Transportation of Remains, Dependents and Effects; Death Accuring Away From Installation or Abroad,* Washington, D.C., Jan. 5, 2009.

109 Department of Defense. DoDD 1300.22, *Mortuary Affairs Policy,* Feb. 3, 2000, 1-10.

110 Department of Defense. DoDD 1300.18, *Department of Defense (DoD) Personnel Casualty Matters, Policies, and Procedures,* Aug. 14, 2009, 13-15. Department of the Army. AR 600-8-1, *Army Casualty Program*, Washington, D.C., Apr. 30, 2007, 3-11; Department of the Navy. MCO P3040.4E, *Marine Corps Casualty Procdecures Manual,* Washington, D.C., Feb. 27, 2003, 3-11; Department of the Navy. MILSPERSMAN 1770, *Casualties and Survivor's Benefits,* Washington, D.C., Feb. 13, 2008, 1-19; Department of the Air Force. AFI 36-3002, *Casualty Service,* Washington, D.C., July 25, 2007, 31-66.

111 Department of Defense. DoDD 1300.22, *Mortuary Affairs Policy,* Feb. 3, 2000, 2, 5; Department of the Army. AR 638-2, *Care and Disposition of Remains and Disposition of Personal Effects,* Washington, D.C., Dec. 22, 2000, 12-24; Department of the Air Force. AFI 34-242, *Mortuary Affairs Program,* Washington, D.C., Apr. 2, 2008, 48-56; DoD Decedent Affairs Manual. *Decedent Affairs Program,* Washington, D.C., Sept. 17, 1987, 2-1, 2-21.

This page intentionally left blank.

Chapter 5
Support to DoD Healthcare Providers

Our healthcare providers play an important role as force multipliers, keeping our fighting force physically and mentally fit. How we handle military mental health affects operational readiness. Our caregivers are not immune to the cumulative psychological effects of persistent conflict. They serve alongside our combat forces where they provide quality care that is second-to-none. They experience, share, and help our troops cope with the fears, grief, and concerns that accompany war against dangerous, tough, and elusive enemies. They often do not avail themselves of access to support resources similar to those that they provide to our fighting forces. Our review suggests that a culture exists in which military healthcare providers are encouraged to deny their own physical, psychological, and social needs to provide the necessary support to beneficiaries. Supporting and sustaining those who care for our forces translates to a healthy workplace, a culture of trust and respect, and caregivers who are invigorated rather than depleted by their intimate professional connections with traumatized patients.

The Department of Defense requires a comprehensive approach to ensure health care readiness—care for both warriors and caregivers.

The Department of Defense requires a comprehensive approach to ensure healthcare readiness—care for both warriors and caregivers. The Department of Defense should consider policies, procedures, and properly resourced programs to preserve our capabilities in this important combat service support area that include:

- leading the health provider force—by providing the senior mentoring and leadership necessary to groom tomorrow's caregivers and establishing proper oversight to provide early warning of both patients and caregivers who may be dangers to themselves and others;
- maintaining the health provider force—by addressing health professionals' readiness, ensuring we retain quality health providers, and developing deployment cycles that allow us to sustain the caregiver force just as we do for our combat and combat support forces;
- resourcing the health provider force—by increasing opportunities for the care and recovery of DoD healthcare providers.

For the purposes of this review, caregivers include healthcare providers and healthcare professionals as defined by the Department of Defense.[112] This group is further augmented with chaplains, medics, corpsmen, and counselors, whether deployed or in garrison.

Mental Health Care Support

Finding 5.1

- DoD installations are not consistent in adequately planning for mental health support for domestic mass casualty incidents to meet needs of victims and families.
- At Fort Hood, advanced treatment protocols developed at our universities and centers were not available to the commander prior to the incident.
- Fort Hood developed a Behavioral Health plan[113] that incorporated current practices including a "whole of community" approach, and a strategy for long-term behavioral healthcare not reflected in any DoD policy.

112 Department of Defense. DoD Manual 6015.1-M, *Glossary of Healthcare Terminology,* January 1999, 75-76.

113 Campaign Plan PC 09-11-655, *Fort Hood Behavioral Health Campaign Plan,* Dec. 7, 2009, 1-2.

Discussion

Current Department of Defense medical policy regarding combat stress does not address traumatic stress response in a domestic mass casualty incident.[114] There are emerging advanced treatment techniques for traumatic stress that should inform DoD policies.

Several DoD programs and initiatives are working to optimize mental healthcare. The most advanced DoD programs or initiatives include the Uniformed Services University of Health Sciences' Center for the Study of Traumatic Stress,[115] the Department of Defense Task Force on Mental Health, and the Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury.[116]

These programs have developed:

- A series of pamphlets entitled "Courage To Care," to inform both patients and providers on a range of disaster mental health concerns.[117]
- A standardized provider training curriculum for treating post traumatic stress disorder.[118]
- Validated practice standards for treating psychological disorders to ensure the Department of Defense meets the needs of the nation's military communities, warriors, and families.[119]
- A series of preventive programs to mitigate development of psychological disorders in the aftermath of disasters.

Although the Department of Defense has not consistently incorporated these best practices into policy, a review of Service policies identified that current practices are reflected in an Air Force Instruction that provides a comprehensive, proactive approach to traumatic stress response.[120]

Recommendation 5.1

- Update Mental Health Care clinical practice guidelines that address both combat and domestic incidents to ensure current and consistent preventive care.
- Review best practices inside and outside the Department of Defense to develop policies, programs, process, and procedures to provide commanders tools required to protect the force in the aftermath of combat or mass casualty incidents.
- Consider the Air Force Instruction and the Fort Hood Behavioral Health Campaign Plan as possible sources for developing appropriate guidance.[121]

---

114 Department of Defense. DoDD 6490.5, *Combat Stress Control Programs,* Washington, D.C., Nov. 24, 2003, 1-9.

115 Uniformed Services University of the Health Services, *Department of Psychiatry,* http://www.usuhs.mil/psy/psychfellowships.html, (accessed Dec 10, 2009).

116 Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury, *For Health Professionals,* http://www.dcoe.health.mil/ForHealthPros.aspx, (accessed Dec. 10, 2009).

117 Uniformed Services University of the Health Sciences. *Courage to Care, Adherence: Addressing a Range of Patient Health Behaviors,* Bethesda, MD; Uniformed Services University of the Health Sciences. *Courage to Care, Staying the Course: Following Medical Recommendations for Health,* Bethesda, MD.

118 Uniformed Services University of the Health Sciences. *"USU Newsletter: Addressing the Psychological Health of Warriors,"* Aug. 4, 2008, 3.

119 Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury, *For Health Professionals,* http://www.dcoe.health.mil/forHealthPros.aspx, (accessed Dec. 8, 2009).

120 Department of the Air Force. AFI 44-153, *Traumatic Stress Response,* Washington, D.C., Mar. 31, 2006, 1-17.

121 Department of the Air Force. AFI 44-153, *Traumatic Stress Response,* Washington, D.C., Mar. 31, 2006, 1-17; Campaign Plan PC 09-11-665, *Fort Hood Behavioral Health Campaign Plan,* Dec 7, 2009, 1-17.

Finding 5.2

- The Department of Defense does not have comprehensive policies that recognize, define, integrate, and synchronize monitoring and intervention efforts to assess and build healthcare provider readiness.
- The Department of Defense 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.
- 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 military personnel and their families from our high operational tempo and repeated assignments in combat areas.

Discussion

The Services have a variety of policies, programs, and specific course content that present concepts on readiness and resilience as it applies to all Service members. Our review of Service policies, information papers, and individual interviews revealed that the emerging resiliency programs are currently described in various documents, but are not yet integrated across Service Doctrine.

Our review revealed that the Department of Defense currently does not endorse a program encompassing all of the desired attributes of a healthcare provider readiness strategy.

Our review revealed that the Department of Defense currently does not endorse a program encompassing all of the desired attributes of a healthcare provider readiness strategy. As the Army and Navy continue to implement their programs, they are using a validated tool to assess effectiveness. This is a step in the right direction. These Services recognize that addressing readiness levels may improve the retention of critically skilled personnel.[122] For those agencies using a monitoring tool, however, little actionable feedback is being provided to leaders to affect program development and sustainment. The use of a common tool would assist interagency and civilian intervention benchmarking, further extending program capability and effectiveness.

There are evolving collaborations between DoD entities and civilian organizations to support healthcare providers. Our review suggests that it continues to be difficult for commanders at local levels to establish formal collaboration on readiness programs due to resource and contracting barriers. Research on the field of secondary trauma suggests that preventive programs designed to provide comprehensive support to enhance resilience and reduce fatigue in behavioral health employees treating mental health problems (e.g., Post Traumatic Stress Disorder) among service personnel are critical. Civilian programs that build on the already strong tradition of buddy systems in the military are particularly valuable.[123]

122 Interview with Coordinator of Mental Health Wellness Programs, Navy Bureau of Medicine and Surgery, Washington, D.C., Dec 10, 2009.

123 Dr. Charlie Benight, University of Colorado at Colorado Springs, National Center for Provider Resilience. *SupportNet Program for Frontline Providers for Traumatic Stress,* Washington, D.C., Dec. 7, 2009.

Recommendation 5.2

Create a body of policies that:

- recognizes, defines, and synchronizes efforts to support and measure healthcare provider readiness in garrison and deployed settings;
- addresses individual assessment, fatigue prevention, non-retribution, and reduced stigma for those seeking care, and appropriate procedures for supporting clinical practice during healthcare provider recovery;
- requires 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;
- develop mechanisms for collaborating with civilian resiliency resources.

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.

Discussion

Healthcare providers experience the transmission of traumatic stress from one individual to another. The Department of Defense Task Force on Mental Health Report noted the importance of enhancing the resiliency and recovery of combatants due to the emotional pathologies of combat.[124] The Services have robust programs for pre- and post-deployment care for their members, but some have only recently initiated similar programs for healthcare providers.[125] It is equally important to enhance the resiliency and recovery of care providers.[126] These programs should be fully integrated, with lessons learned and best practices. The Services appear to have insufficient data to assess traumatic stress and healthcare provider burnout, critical elements in assessing stress control programs for the force. Programs for chaplains and others who support the religious ministry are notable for their comprehensive scope and effectiveness.

Despite the efforts of the Services, there is ongoing hesitancy among healthcare providers to seek treatment when they experience stress related to their roles as care providers. The professional ethic favors placing patient and organizational needs above personal health and emotional concerns.

Our healthcare readiness approach should balance the needs of patients with the needs of the providers. An example of a well-intentioned program that may have unintended consequences for our healthcare providers is the Army's requirement for specific caregivers assigned to deployed Brigade Combat Teams to remain in their currently assigned Brigade Combat Teams for a minimum of 90 days after return from deployment. While providing continuity of care for returning soldiers, this may delay care provider recovery.[127]

124 VADM Donald C. Arthur, USN, Shelley MacDermid, and LTG Kevin C. Kiley, USA. Washington, D.C., 2007.

125 Department of the Navy. Draft, 091104. *Combat and Operational Stress Control,* Washington, D.C., unpublished; LTC Steve Lewis, PhD, USA. Briefing to Chief of Staff of the Army. *MEDCOM Provider Resiliency Training (PRT) Program,* Dec 7, 2009.

126 Ibid.

127 ALARACT 214/2009, *Stop Loss and Deployment Policy Updates,* Aug. 4, 2009, 1-5.

Chapter 5
Support to DoD Healthcare Providers

Demand for healthcare support continues to increase. With high operational tempo and repeat tours in combat areas, the need for healthcare support will not level, much less diminish, in the foreseeable future. The superb care our military personnel and their families have received will be increasingly at risk if issues identified in this report are not resolved quickly in an integrated, comprehensive manner.

Recommendation 5.3

- Develop integrated policies, processes, procedures, and properly resourced programs to sustain high quality care.
- 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.
- Review the requirement for the Department of Defense to de-stigmatize healthcare providers who seek treatment for stress.

Finding 5.4

Senior caregivers are not consistently functioning as clinical peers and mentors to junior caregivers.

Discussion

Providing strong mentor relationships among healthcare providers and retaining experienced senior expertise at the clinical level are vital elements in providing quality healthcare. Current Service career patterns, with some recent innovative efforts as important exceptions, move senior clinicians away from patient care to career-enhancing leadership positions. This leaves junior clinicians and support staff without the assistance of seasoned clinicians. This limited daily interaction with clinically- and militarily-experienced mentors can hamper force development. The Army and the Navy have demonstrated a commitment to keep highly-trained academic physicians in the Medical Treatment Facilities for prolonged tours. The Air Force has developed an O-6 Senior Clinician Billet program to place senior physicians back in full-time clinical practice to serve as mentors and to share clinical expertise. These experienced providers serve as reassuring role models and advisors to less experienced coworkers.[128]

The retention of experienced clinicians in the Services is a concern. While addressing the retention issue is beyond the scope of this inquiry, it should be noted that dissatisfaction with healthcare provider support can be identified as a negative influence on career longevity. For example, data from the recent Air Force Medical Corps Exit Survey (while not fully representative or generalized) identifies clinical, deployment, and administrative demands placed on physicians as common influences on decisions to separate from the Air Force Medical Service.[129] As previously addressed, these demands may affect the Services' abilities to integrate incentives to support provider readiness. The downward trajectory continues when providers are surrounded by teammates whose focus is on exiting the Service.

Recommendation 5.4

Review Senior Medical Corps Officer requirements to determine optimal roles, utilization, and assignments.

128 Col Arynce Pock, USAF, AF/SG1, "Position Description: O-6 Clinician," Dec. 14, 2009.

129 Col Arynce Pock, USAF, AF/SG 1M, email to Lt Col Janice Langen, USAF, Dec. 16, 2009.

This page intentionally left blank.

Appendix A
Memorandum and Terms Of Reference

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

NOV 20 2009

MEMORANDUM FOR THE HONORABLE TOGO WEST
ADMIRAL VERN CLARK, U.S. NAVY (RET.)

SUBJECT: Independent Panel for Department of Defense Review Related to Fort Hood

Thank you for agreeing to serve as Co-Chairs for DoD's Independent Review related to Fort Hood. In this capacity, I ask that you conduct the Review to identify and address possible gaps and/or deficiencies in the DoD's programs, processes, and procedures related to identifying DoD employees who could potentially pose credible threats to themselves or others; the sufficiency of DoD's force protection programs; and the sufficiency of the DoD's emergency response to mass casualty situations at DoD facilities and the response to care for victims and Families in the aftermath of a mass casualty situation. Also, you are to assess the execution and adequacy of Army programs, policies, and procedures as applied to the alleged perpetuator.

The President has directed a review of intelligence matters related to the Fort Hood shooting, and a military justice investigation is underway. It is critical to maintain the integrity of these investigations. Therefore, your review should not interfere with either of these activities. It is also important to state that nothing herein should be interpreted as expressing any view on the culpability of any individual for the events of November 5, 2009.

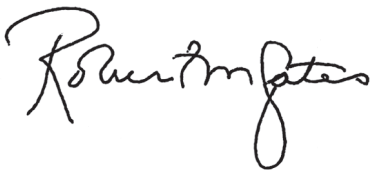
The prime objective of this Review is to determine whether there are programs, policies or procedural weaknesses within DoD that create vulnerabilities to the health and safety of our employees and their families. Your terms of reference are attached.

I appoint you as full-time employees of DoD using the applicable authorities available to me. You are to have access to all relevant DoD investigations and other DoD information unless prohibited by law or this memorandum. Reviewing all written materials relevant to these issues may be sufficient to allow you to provide your independent advice. Should you identify the need to travel or conduct interviews, the Acting Director of Administration and Management will make appropriate arrangements.

You are to begin the Review on November 20, 2009, with a report, including findings and recommendations, provided to me by January 15, 2010. You may identify follow-on issues which may require further study. At the conclusion of this Review, the Secretary of Defense will task each Service and pertinent DoD agencies to conduct an in-depth follow-on review, based on the findings of the report.

By copy of this memorandum, I request that the Acting Director of Administration and Management secure the necessary technical, administrative, and legal support for your review from DoD Components. Furthermore, the Acting Director of Administration and Management will provide administrative, facilities, and other support, as required.

Lastly, all DoD Components will fully cooperate in the execution of this Review and be responsive to all requests for relevant information, detailed personnel, or other support so that the Review Panel may deliver its independent findings and recommendations to me not later than January 15, 2010.



Attachment(s):
As stated

cc:
Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
Assistant Secretaries of Defense
General Counsel of the Department of Defense
Inspector General of the Department of Defense
Acting Director of Administration and Management

TERMS OF REFERENCE
Department of Defense (DoD) Independent Review Relating to Fort Hood

These Terms of Reference (TOR) cover the objectives of the Secretary of Defense-directed a DoD Independent Review relating to Fort Hood (hereafter referred to as "the Review") related to the November 5, 2009 mass shooting at Fort Hood, Texas. The Review will identify and address possible gaps and/or deficiencies in the DoD's programs, processes, and procedures related to identifying Department employees who could potentially pose credible threats to themselves or others; the sufficiency of DoD's force protection programs; and the sufficiency of the DoD's emergency response to mass casualty situations at DoD facilities and the response to care for victims and Families in the aftermath of a mass casualty situation.; and assess the execution and adequacy of Army programs, policies, and procedures as applied to the alleged perpetuator.

The prime objective of this Review is to determine whether there are programs, policies or procedural weaknesses within DoD that create vulnerabilities to the health and safety of our employees and their families.

The TOR includes background information, objectives and scope, methodology, duration and limitations and deliverables.

Background:

The shooting that occurred on November 5, 2009, at the Soldier Readiness Center of Fort Hood Texas, resulted in the deaths of 12 soldiers and one Army civilian. Thirty others with gunshot wounds were hospitalized.

The President has directed a review of intelligence matters related to the Fort Hood shooting, and a military justice investigation is underway. It is critical to maintain the integrity of these investigations. Therefore, this review should not interfere with either of these activities. It is also important to state that nothing herein should be interpreted as expressing any view on the culpability of any individual for the events of November 5, 2009.

Objectives and Scope:

The Review will identify and address possible gaps and deficiencies in the areas reflected below:

- Programs, processes and procedures related to identifying Department employees who could potentially pose credible threats to others. This includes, but is not limited to:
    - Personal reliability programs;
    - Periodic counseling sessions;

- Reporting and handling of Department employees adverse information procedures;
- Service Member release and discharge policies and procedures;
- Medical screening programs to determine
  - Initial suitability prior to specialization
  - Follow-on/ongoing screening once an individual has been selected;
- Pre and post-deployment health assessment programs.
- Personnel evaluations.

- Sufficiency of DoD's force protection programs.

- Sufficiency of the DoD's emergency response to mass casualty situations at DoD facilities and the response to care for victims and Families in the aftermath of a mass casualty situation.

- Assess the execution and adequacy of Army programs, policies, and procedures as applied to the alleged perpetuator.

- Assess whether Army and other programs, policies, and procedures functioned properly across the alleged perpetrator's career as a military health care provider, to retain and promote him in the Army Medical Corps.

- Assess whether Army programs, policies, and procedures governing the release or discharge from the Army of personnel determined not to be fully qualified, or to be unsuitable for, continued military service (without regard to whether the individual is subject to a continuing service obligation), functioned appropriately as applied to the alleged perpetrator.

- Assess the adequacy of Army programs, policies, and procedures for the support and care of health care providers while involved with the provision of health care directly to beneficiaries suffering from Post Traumatic Stress Disorder or other mental and emotional wounds and injuries.

- Assess whether the care provided by the alleged perpetrator to patients and former patients met accepted standards.

Methodology:

- Review all DoD directives, instructions, and other issuances with potential impact on subject review.

- Conduct interviews as necessary with appropriate senior officials (health affairs, law enforcement and force protection, first responders, intelligence), peer and subordinate groups, witnesses, and other pertinent individuals.

- Formulate recommendations for correcting problems identified and enhancing internal controls to preclude future incidents/mitigate associated risk.

Duration:

The Review will begin on November 20, 2009. A report with findings and recommendations will be provided to the Secretary of Defense by January 15, 2010. At the conclusion of this Review, the Secretary of Defense will task each Service and pertinent DoD agencies to conduct an in-depth follow-on review, based on the findings of the report. Follow-on issues may be identified during the course of the initial review and pursued, subject to approval.

Deliverables:

- The Independent Review Panel will provide a report to the Secretary of Defense by January 15, 2010 that addresses the areas discussed above.

- The Review will provide actionable recommendations to improve current programs, process and procedures, if warranted.

Support:

- The Under Secretary of Defense (Comptroller)/Chief Financial Officer will provide adequate funding for the Review.

- The Acting DA&M, through Washington Headquarters Services, will coordinate for and provide human resources, office/facilities, and other support, as required, to ensure success of this effort.

- The Review will be able to draw upon the full support of the Military Departments and other DoD Components for support, personnel, information (including but not limited to documents and interviews personnel), and analytical and investigative capacity as determined necessary by the Co-Chairs.

This page intentionally left blank.

Appendix B
Panel Roster

Executive Director
Col David Krumm, USAF

Director of Staff
Lt Col Donna Turner, USAF

Panel Staff
Mr. James Schwenk
CAPT Donald Gabrielson, USN
CDR John Rickards, USN
CDR Shawn Malone, USN
LTC James Clemonts, USA
Lt Col Rhonda Ozanian, USAF
Lt Col Charlie Underhill, USAF
LTC Heather Kness, USA
LtCol Matthew Phares, USMC
LTC Jonathan Withington, USA
MAJ Jonathan Due, USA
MAJ Bryan Price,PhD, USA
MSgt Tarri Long, USAF
Mr. Benjamin Bryant
Anthony C. Cain, PhD
Ms. Dorothy Hale
Ms. Desiree Parker
Ms. Liza Vivaldi
Mr. Thomas Zamberlan

Red Team
Ms. Sally Donnelly, *Team Lead*
CDR David Copp, USN
Mr. Howard Luker
Mr. James Mitchell
Frances Murphy, MD, MPH

Personnel Policies and Procedures
Gen Stephen Lorenz, USAF, *Team Lead*
COL (P) Billy D. Farris, USA, *Deputy*
Mr. James Neighbors, SES, *Chief of Staff*
BG Peter Zwack, USA
Col Dave Wesley, USAF
COL David Lemauk, USA
Chap (Col) Jerry Pitts, USAF
Lt Col Susanne Wheeler, USAF
LTC Teresa Gaborik, USA
LTC Brian Mack, USA
Maj David O'Malley, USAF
Maj Joshua Morganstein, USAF
Chap (LCDR) Charles Varsogea, USN
Capt Marrisa Carlton, USAF
SgtMaj William Skiles, USMC
MSG Stuart Coupe, USA
PSC Melanie Kinchen, USN
Mr. Marc A. Blincoe
Ms. Lynn Borkon
Mr. Fred Bryant
Ms. Victoria Darwin
Maren Leed, PhD
Ms. Melissa Lopez
Laura Miller, PhD
Mr. Dorian Sajona
Ms. Marcella Sandiford
Mr. George Truss

Force Protection
RADM Mark Buzby, USN, *Team Lead*
Mr. Raymond Geoffroy, SES, *Deputy*
CAPT Chris Kiley, USN, *Chief of Staff*
Lt Col Eric Knapp, USAF
Ms. Lisa Burgess
Mr. James Cain
Mr. Michael Dickey
Mr. Kevin Dodds
Ms. Rhonda Gayle
Mr. Kevin Naylon
Mr. Eugene Smith
Mr. John Gregory Steele
Mr. Thaldaris Talley
Mr. John Vesterman

Emergency Management & Response
LtGen Frank Panter, USMC, *Team Lead*
Brig Gen Jeffery Lofgren, USAF, *Deputy*
Capt Jay Montgomery, USMC, *Chief of Staff*
CH (COL) Clark McGriff, USA
COL Knickerbocker, USA
COL Kathleen Ford, USA
CDR Sawsan Ghurani, USN
CDR Eric Runnels, USCG

Charles Beadling, MD
Ms. Cheryl Hackley
Mr. Owen McIntyre
Mr. Todd Rose
Mr. Thomas Ruffini
Mr. Randy Smith
Mr. Mark Ward
Ms. Gabriela Wilson

Application of Policies and Procedures
GEN Carter Ham, USA, *Team Lead*
MG Bill McCoy, USA, *Deputy*
Mr. James Neighbors, SES, *Chief of Staff*
Maj Gen Thomas Travis, USAF
Brig Gen Eden Murrie, USAF
Col James Black, USAF
COL Cornelius Maher, USA
COL Doreen Lounsbery, USA
Col Christopher O'Brien, USAF
Col Gerald Talcott, USAF
Lt Col Bill Fischer, USAF
LTC Christopher Carrier, USA
Maj Dan Janning, USAF
Maj Elizabeth Greene, USAF
MAJ Wesley Howard, USA
Capt Sarah Carpenter, USAF
Ms. Sonja Ackar
Mr. Bruce Barry
Ms. Ellen Campana
Mr. Edgar Collins
Mr. Hal Dronberger
Mr. James Fazio
Ms. Georganna Murto
Mr. Hung Nguyen
Ms. Amanda Smith
Ms. Debra Tolson
Mr. Carl Witcher

Care for Healthcare Providers
RADM Karen Flaherty, USN, *Team Lead*
CH (COL) John Read, USA, *Deputy*
CDR Anne Swap, USN, *Chief of Staff*
COL Kelly Wolgast, USA
Lt Col Janice M. Langer, MD, USAF
CDR Rosemary Carr Malone, MD, USN
CDR Barry Adams, PhD, LCSW, USN
Lt Col Teresa Roberts, LCSW, USAF
MAJ Todd Yosick, USA
LCDR James Cannon, PhD, PA, USCG
SGM Devon Matthew, USA
SMSgt Glynda Lilly, USAF
Mr. Dale Hamby
Ms. Mary Woodward

Appendix C
Summary of Findings and Recommendations

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

- Update training and education programs to help DoD personnel identify contributing factors and behavioral indicators of potentially violent actors.
- Coordinate with the FBI Behavioral Science Unit's Military Violence unit to identify behavioral indicators that are specific to DoD personnel.
- Develop a risk assessment tool for commanders, supervisors, and professional support service providers to determine whether and when DoD personnel present risks for various types of violent behavior.
- Develop programs to educate DoD personnel about indicators that signal when individuals may commit violent acts or become radicalized.

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

- Evaluate background check policies and issue appropriate updates.
- Review the appropriateness of the depth and scope of the National Agency Check with Local Agency and Credit Check as minimum background investigation for DoD SECRET clearance.
- Educate commanders, supervisors, and legal advisors on how to detect and act on potentially adverse behaviors that could pose internal threats.
- Review current expedited processes for citizenship and clearances to ensure risk is sufficiently mitigated.

Finding 2.3

DoD standards for denying requests for recognition as an ecclesiastical endorser of chaplains may be inadequate.

Recommendation 2.3

Review the limitations on denying requests for recognition as ecclesiastical endorsers of chaplains.

Finding 2.4

The Department of Defense has limited ability to investigate Foreign National DoD military and civilian personnel who require access to DoD information systems and facilities in the U.S. and abroad.

Recommendation 2.4

Coordinate with the Department of State and Office of Personnel Management to establish and implement more rigorous standards and procedures for investigating Foreign National DoD personnel.

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

- Assess whether pre- and post-deployment behavioral screening should include a comprehensive violence risk assessment.
- Review the need for additional post-deployment screening to assess long-term behavioral indicators that may point to progressive indicators of violence.
- Revise pre- and post-deployment behavioral screening to include behavioral indicators that a person may commit violent acts or become radicalized.
- 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.

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

- Revise current policies and procedures to address preventing violence toward others in the workplace.
- 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.

Finding 2.7

DoD policy regarding religious accommodation lacks the clarity necessary to help commanders distinguish appropriate religious practices from those that might indicate a potential for violence or self-radicalization.

Recommendation 2.7

Promptly establish standards and reporting procedures that clarify guidelines for religious accommodation.

Summary of Findings and Recommendations

Finding 2.8

DoD Instruction 5240.6, *Counterintelligence (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

Update DoD Instruction 5240.6 to provide specific guidance to the Services, Combatant Commands, and appropriate agencies for counterintelligence awareness of the full spectrum of threat information particularly as it applies to behavioral indicators that could identify self-radicalization.

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

- 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.
- Develop supporting policies and procedures for commanders and supervisors to access this information.

Finding 2.10

There is no consolidated criminal investigation database available to all DoD law enforcement and criminal investigation organizations.

Recommendation 2.10

Establish a consolidated criminal investigation and law enforcement database such as the Defense Law Enforcement Exchange.

Finding 2.11

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

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, with clearly established standards regarding scope and timeliness.

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 2.12

Ensure Services update policies to reflect current DoD-level guidance on the release of protected health information.

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

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.

Finding 2.14

The Department of Defense does not have a comprehensive and coordinated policy for counterintelligence 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 counterintelligence collection, investigations, and operations in cyberspace for identifying potential threats to DoD personnel, information, and facilities.

Finding 2.15

DoD policy governing prohibited activities is unclear and does not provide commanders and supervisors the guidance and authority to act on potential threats to good order and discipline.

Recommendation 2.15

Review prohibited activities and recommend necessary policy changes.

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.

Summary of Findings and Recommendations

Recommendation 2.16

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.

Finding 3.1

- The Department of Defense has not issued an integrating force protection policy.
- Senior DoD officials have issued DoD policy in several force protection-related subject areas such as antiterrorism but these policies are not well integrated.

Recommendation 3.1

- Assign a senior DoD official responsibility for integrating force protection policy throughout the Department.
- Clarify geographic combatant commander and military department responsibilities for force protection.
- Review force protection command and control relationships to ensure they are clear.

Finding 3.2

DoD force protection programs and policies are not focused on internal threats.

Recommendation 3.2

- Develop policy and procedures to integrate the currently disparate efforts to defend DoD resources and people against internal threats.
- 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 relating to pending violence.
- Provide commanders with a multidisciplinary capability, based on best practices such as the Navy's Threat Management Unit, the Postal Service's "Going Postal Program," and Stanford University's workplace violence program, focused on predicting and preventing insider attacks.

Finding 3.3

The Department of Defense's commitment to support JTTFs is inadequate.

Recommendation 3.3

- Identify a single point of contact for functional management of the Department of Defense's commitment to the JTTF program.
- 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.
- Review the commitment of resources to the JTTFs and align the commitment based on priorities and requirements.

Finding 3.4

There is no formal guidance standardizing how to share Force Protection threat information across the Services or the Combatant Commands.

Recommendation 3.4

Direct the development of standard guidance regarding how military criminal investigative organizations and counterintelligence organizations will inform the operational chain of command.

Finding 3.5

The Department of Defense does not have direct access to a force protection threat reporting system for suspicious incident activity reports.

Recommendation 3.5

- Adopt a common force protection threat reporting system for documenting, storing, and exchanging threat information related to DoD personnel, facilities, and forces in transit.
- Appoint a single Executive Agent to implement, manage, and oversee this force protection threat reporting system.

Finding 3.6

There are no force protection processes or procedures to share real-time event information among commands, installations, and components.

Recommendation 3.6

Evaluate the requirement for creating systems, processes, policy, and tools to share near real-time, unclassified force protection information among military installations in CONUS to increase situational awareness and security response.

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

- Review best practices, including programs outside the U.S. Government, to determine whether elements of those programs could be adopted to augment access control protocols to detect persons who pose a threat.
- Review leading edge tools and technologies that augment physical inspection for protecting the force.

Finding 3.8

The Department of Defense does not have a policy governing privately owned weapons.

Recommendation 3.8

Review the need for DoD privately owned weapons policy.

Finding 3.9

Services cannot share information on personnel and vehicles registered on installations, installation debarment lists, and other relevant information required to screen personnel and vehicles, and grant access.

Recommendation 3.9

- Develop timely information sharing capabilities among components including vehicle registration, installation debarment lists, and other access control information.
- Accelerate efforts to automate access control that will authenticate various identification media (e.g., passports, CAC, drivers' licenses, license plates) against authoritative databases.
- Obtain sufficient access to appropriate threat databases and disseminate information to local commanders to enable screening at CONUS and overseas installation access control points.

Finding 4.1

Services are not fully interoperable with all military and civilian emergency management stakeholders.

Recommendation 4.1

- Establish milestones for reaching full compliance with the Installation Emergency Management program.
- Assess the potential for accelerating the timeline for compliance with the Installation Emergency Management program.

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

Develop policy that provides implementation guidance for Enhanced 911 services in accordance with applicable laws.

Finding 4.3

DoD policy does not currently take advantage of successful models for active shooter response for civilian and military law enforcement on DoD installations and facilities.

Recommendation 4.3

- Identify and incorporate civilian law enforcement best practices, to include response to the active shooter threat, into training certifications for civilian police and security guards.
- Include military law enforcement in the development of minimum training standards to ensure standard law enforcement practices throughout the Department of Defense.
- 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.
- Develop a case study based on the Fort Hood incident to be used in installation commander development and on-scene commander response programs.

Finding 4.4

Based on Joint Staff Integrated Vulnerability Assessments, many DoD installations lack mass notification capabilities.

Recommendation 4.4

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.

Finding 4.5

Services have not widely deployed or integrated a Common Operational Picture capability into Installation Emergency Operations Centers per DoD direction.

Recommendation 4.5

- Examine the feasibility of accelerating the deployment of a state-of-the-art Common Operational Picture to support installation Emergency Operations Centers.
- Develop an operational approach that raises the Force Protection Condition 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.

Finding 4.6

- Stakeholders in the DoD Installation Emergency Management program, including the Under Secretary of Defense for Policy; Under Secretary for Personnel and Readiness; Under Secretary of Defense for Intelligence; Under Secretary of Defense for Acquisition, Technology & Logistics; Assistant Secretary of Defense for Public Affairs; and Assistant Secretary of Defense for Networks

and Information Integration/Chief Information Officer, have not yet synchronized their applicable programs, policies, processes, and procedures.

- Better synchronization and coordination would remove redundant planning requirements, identify seams in policy, focus programmed resources, and streamline procedures to achieve unity of effort in installation emergency management.

Recommendation 4.6

- Review responsibilities for synchronizing Office of the Secretary Defense programs, policies, and procedures related to installation emergency management.
- Establish policy requiring internal synchronizing of installation programs, plans, and response for emergency management.

Finding 4.7

Mutual Aid Agreements (MAAs) between DoD and civilian support agencies across the Services are not current.

Recommendation 4.7

Review Installation Emergency Management programs to ensure correct guidance on integrating tracking, exercising, and inspections of MAAs.

Finding 4.8

The Department of Defense 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

- Develop guidance incorporating the core service elements of a Family Assistance Center as identified in the Pentagon AAR.
- Develop implementation guidance to establish requirements for a Family Assistance Center crisis and mass casualty response as integral components of Installation Emergency Management plans.
- Consider the Air Force's Emergency Family Assistance Control Center and the Fort Hood Behavioral Health Campaign Plan as possible best practices when developing policy.

Finding 4.9

The lack of published guidance for religious support in mass casualty incidents hampers integration of religious support to installation emergency management plans.

Recommendation 4.9

- 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.
- Develop policy for religious support in response to mass casualty incidents and integrate guidance with the Installation Emergency Management Program.

Finding 4.10

Inconsistencies among Service entry level chaplain training programs can result in inadequate preparation of new chaplains to provide religious support during a mass casualty incident.

Recommendation 4.10

Review mass casualty incident response training in the Chaplain Basic Officer Courses.

Finding 4.11

The Department of Defense 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

Develop standardized policy guidance on memorial service entitlements.

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

- 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.
- Review current mortuary affairs policies relating to mortuary services for private citizens who become fatalities on a military installation within CONUS.

Finding 5.1

- DoD installations are not consistent in adequately planning for mental health support for domestic mass casualty incidents to meet needs of victims and families.
- At Fort Hood, advanced treatment protocols developed at our universities and centers were not available to the commander prior to the incident.
- 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.

Summary of Findings and Recommendations

Recommendation 5.1

- Update Mental Health Care clinical practice guidelines that address both combat and domestic incidents to ensure current and consistent preventive care.
- Review best practices inside and outside the Department of Defense 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.
- Consider the Air Force Instruction and the Fort Hood Behavioral Health Campaign Plan as possible sources for developing appropriate guidance.

Finding 5.2

- The Department of Defense does not have comprehensive policies that recognize, define, integrate, and synchronize monitoring and intervention efforts to assess and build healthcare provider readiness.
- The Department of Defense 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.
- 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 military personnel and their families from our high operational tempo and repeated assignments in combat areas.

Recommendation 5.2

Create a body of policies that:

- recognizes, defines, and synchronizes efforts to support and measure healthcare provider readiness in garrison and deployed settings;
- addresses individual assessment, fatigue prevention, non-retribution, and reduced stigma for those seeking care, and appropriate procedures for supporting clinical practice during healthcare provider recovery;
- requires 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;
- develop mechanisms for collaborating with civilian resiliency resources.

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

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

- 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.
- Review the requirement for the Department of Defense to de-stigmatize healthcare providers who seek treatment for stress.

Finding 5.4

Senior caregivers are not consistently functioning as clinical peers and mentors to junior caregivers.

Recommendation 5.4

Review Senior Medical Corps Officer requirements to determine optimal roles, utilization, and assignments.

Appendix D
Literature Review of Risk Factors for Violence

This Appendix highlights some major themes in the academic literature, based primarily on literature reviews from 2000 – the present. Within categories of violence (e.g., suicide, terrorism, sexual violence), researchers have sought ways to distinguish those who carry out acts of violence from those who do not. Researchers also have studied particular risk factors (e.g., substance abuse, mental illness) to determine which types of violence are associated with specific risk factors and why.[1] Overarching themes on risk factors for violence toward self or others include the following:

Predicting Violent Behavior is a Long-Term Multi-Disciplinary Quest

Researchers have yet to develop a single model that can estimate who is at risk for any type of violence, but they have made progress on models to identify risks for particular forms of violence, or specific populations, such as psychiatric patients.[2]

Most research to date has been conducted on physical violence perpetrated by individuals.[3] No field has substantiated the image of violence emerging from a normal, happy, healthy individual who suddenly "snaps" in the face of a single triggering event. In addition, no single variable has been identified that can accurately predict violence.

Identifying potentially dangerous people before they act is difficult. Examinations after the fact show that people who commit violence usually have one or more risk factors for violence. Few people in the population who have risk factors, however, actually assault or kill themselves or others. For example, many people experience depression, but relatively few attempt or die by suicide. Most people who commit violence are male, but most males do not commit violence. Exposure to childhood violence may increase the likelihood that someone may harm themselves or others, but it is not inevitable. Certain combinations of risk factors, however, can significantly increase the likelihood that individuals will become violent.

Risk Factors Vary Across Types of Violence

The range of contributing factors for different types of violence is diverse. Although some factors, such as low self-esteem, depression, and anger are tied to many different types of violence, others are more particular to specific types of aggression. DoD policies and programs that focus on the risk factors for only a few types of violence miss indicators of other types of violence that threaten its community.

---

1 Trevor Bennett, Katy Holloway, and David Farrington, "The Statistical Association Between Drug Misuse and Crime: A Meta-Analysis," *Aggression and Violent Behavior* 13 (2008): 107-118; Eric B. Elbogen and Sally C. Johnson, "The Intricate Link Between Violence and Mental Disorder: Results From the National Epidemiologic Survey on Alcohol and Related Conditions," *Archives of General Psychiatry* 66:2 (2009): 152-161; Seena Fazel, Johanna Philipson, Lisa Gardiner, Rowena Merritt, and Martin Grann, "Neurological Disorders and Violence: A Systematic Review and Meta-Analysis with a Focus on Epilepsy and Traumatic Brain Injury," *Journal of Neurology* 256 (2009): 1591-1602; Christopher J. Ferguson and Kevin M. Beaver, "Natural Born Killers: The Genetic Origins of Extreme Violence," *Aggression and Violent Behavior* 14:5 (2009):286-294; Andrew Harris, and Arthur J. Lurigio, "Mental Illness and Violence: A Brief Review of Research and Assessment Strategies," *Aggression and Violent Behavior* 12 (2007): 542-551; Robert MacCoun, Beau Kilmer, and Peter Reuter, "Research on Drugs-Crime Linkages: The Next Generation," *Toward a Drugs and Crime Research Agenda for the 21st Century:* U.S. Department of Justice, National Institute of Justice (2003).

2 Mary Ann Campbell, Sheila French, and Paul Gendreau, "The Prediction of Violence in Adult Offenders: A Meta-Analytic Comparison of Instruments and Methods of Assessment," *Criminal Justice and Behavior* 35:6 (2009): 567-590; Mark E. Olver, Keira C. Stockdale, and J. Stephen Wormith, "Risk Assessment With Young Offenders: A Meta-Analysis of Three Assessment Measures," *Criminal Justice and Behavior* 36:4 (2009): 329-353; E. Fuller Torrey, John Monahan, Jonathan Stanley, Henry J. Steadman, and the MacArthur Study Group, "The MacArthur Violence Risk Assessment Study Revisited: Two Views Ten Years After Its Initial Publication," *Psychiatric Services* 59:2 (2008): 147-152.

3 Mary R. Jackman, "Violence in Social Life," *Annual Review of Sociology* 28 (2002): 387-415.

The following overview of risk factors illustrates why DoD personnel need more than a simple checklist to determine whether someone may become violent:

Each year, more than one million people in the U.S. are harmed by workplace violence, and an estimated 17,000 take their own lives in their place of employment.[4] The portrait of the "disgruntled" employee who "goes postal" and kills a supervisor does not encompass the full array of workplace homicides: customers, clients, peers, and superiors are also responsible. The rates of workplace violence in the U.S. Postal Service are actually lower than in the general workforce, so that organization, despite the popular phrase, does not provide a "worst case" for study.

Attempts to use personality tests to screen out potentially violent employees at entry have been unreliable. In addition, research has not yet established a link between mental illness and workplace violence.[5] Other behavioral indicators have been identified, however. For example, those who commit workplace violence often believe they have been wronged, such as having been denied service or subjected to a poorly handled lay-off or firing.[6]

Although domestic terrorism is far more common than international terrorism, research on terrorism focuses on the latter.[7] Motivations for domestic terrorism are diverse, and include animal rights, environmentalism, nationalism, white supremacy, religious causes, and right-wing politics.[8] Overall, acts of domestic terrorism tend to occur in large urban areas and target the police and military forces.[9]

Recent research has focused on why individuals become terrorists.[10] Although some people self-radicalize as individuals, more commonly small groups of people self-radicalize together.[11] Group dynamics can foster the dehumanization of targets and the drive to commit violence.[12] In addition, the path to terrorism often involves some real or perceived rewards for participation, the desire to address grievances, and a passion for change.[13]

As with workplace violence, mental illness has not been identified as a contributing factor in the path to terrorism.[14] Furthermore, terrorists are not particularly poor or uneducated.[15]

---

4 Gregory M. Vecchi, "Conflict & Crisis Communication: Workplace and School Violence, Stockholm Syndrome, and Abnormal Psychology," *Annals of the American Psychotherapy Association* 12:3 (2009): 30-39.

5 Julian Barling, Kathryne E. Dupré, and E. Kevin Kelloway, "Predicting Workplace Aggression and Violence," *Annual Review of Psychology* 60 (2009): 671-692.

6 Barling, Dupré and Kelloway, 671-692.

7 Ignacio Sánchez-Cuenca and Luis de la Calle, "Domestic Terrorism: The Hidden Side of Political Violence," *Annual Review of Political Science* 12 (2009): 31-49.

8 Samuel Nunn, "Incidents of Terrorism in the United States, 1997-2005," *Geographical Review* 97:1 (2007): 89-111.

9 Samuel Nunn, "Incidents of Terrorism in the United States, 1997-2005," *Geographical Review* 97:1 (2007): 89-111; Ignacio Sánchez-Cuenca and Luis de la Calle, "Domestic Terrorism: The Hidden Side of Political Violence," *Annual Review of Political Science* 12 (2009): 31-49; Brent Smith, "A Look at Terrorist Behavior: How They Prepare, Where They Strike," *NIJ Journal* 260 (2008): 2-6.

10 Paul K. Davis and Kim Cragin, eds. *Social Science for Counterterrorism* (Santa Monica: RAND, 2009); Austin T. Turk, "Sociology of Terrorism," *Annual Review of Sociology* 30 (2004): 271-286.

11 Todd C. Helmus, "Why and How Some People Become Terrorists," in Davis and Cragin, eds: *Social Science for Counterterrorism* (Santa Monica: RAND, 2009), 71-111.

12 Ibid.

13 Ibid.

14 Ibid.

15 Ibid.

Religious fundamentalism alone is not a risk factor; most fundamentalist groups are not violent, and religious-based violence is not confined to members of fundamentalist groups.[16]

Violence against family members is more common than violence against strangers. Although the factors leading to domestic violence, child abuse, and elder abuse are not identical, key factors in common include: prior aggression, being a victim of or witnessing violence in childhood, low impulse control, low self esteem, poor relationship and communication skills, substance abuse, low income, stress, mental health problems, and antisocial behaviors/ antisocial personality disorder.[17] The risk for intimate partner homicides is higher in homes with domestic violence, firearms, and illicit drug use.[18] Most murder-suicides involve a middle-aged or older man (nearly 100 percent male) using a firearm to kill his current or former wife or girlfriend and then himself, often after the couple has recently separated or there is a pending estrangement.[19] Rates of depression are higher in these cases than in cases of homicide alone, but rates of substance abuse or previous criminal behavior were lower.[20]

Studies of suicide highlight the risk factors of particular mental illnesses, substance abuse, previous suicide attempts, exposure to suicide, social isolation, major physical illnesses, poor impulse control, history of aggression, trauma, or abuse.[21] Some events such as divorce, loss of a job, or death of a loved one, may trigger suicide in those who are already vulnerable.

People who commit sexual violence are diverse, but researchers and law enforcement organizations have created typologies for various forms of sexual violence.[22] These typologies assist with the recognition, investigation, and treatment of sexual offenders. Although there is variation in motivation and methods, rapists tend to share some characteristics, such as negative views of women, hyper-identification with the masculine role, low self esteem, substance abuse problems, and problems managing aggression.[23] Common characteristics of child molesters are poor social skills, low self-esteem, problems forming adult relationships, and a pattern of "grooming" children with manipulative behavior so they will be compliant.[24]

Cyber offenders represent a new category of assailant, following the rise of the Internet and its use by sexual predators to identify and groom children. Female sex offenders have received less attention, and have been treated as their own category due to the difference in characteristics: women are less likely to use force, begin offending at an earlier age (although are less likely to have begun in childhood), and are

16 Michael O. Emerson, and David Hartman, "The Rise of Religious Fundamentalism," *Annual Review of Sociology* 32 (2006): 127-144.

17 Patrick Tolan, Deborah Gorman-Smith, and David Henry, "Family Violence," *Annual Review of Psychology* 57 (2006): 557-583.

18 Lorena Garcia, Catalina Soria and Eric L. Hurwitz, "Homicides and Intimate Partner Violence: A Literature Review," *Trauma, Violence & Abuse* 8: 4 (2007): 370-383.

19 Scott Eliason, "Murder-Suicide: A Review of the Recent Literature," *The Journal of the American Academy of Psychiatry and Law* 37:3 (2009): 371-376; Marieke Liem, "Homicide Followed By Suicide: A Review," *Aggression and Violent Behavior* (2009), doi:10.1016/j.avb.2009.10.001.

20 Eliason, 371-376.

21 Risk and Protective Factors for Suicide, Suicide Prevention Resource Center (SAMHSA) 2009, http://www.sprc.org/suicide_prev_basics/index.asp. [Original source: the *National Strategy for Suicide Prevention: Goals and Objectives for Action* (2001).

22 (Oliver) Heng-Choon Chan, and Kathleen M. Heide, "Sexual Homicide: A Synthesis of the Literature," *Trauma, Violence & Abuse* 10:1 (2009): 31-54.

23 Gina Robertiello and Karen J. Terry, "Can We Profile Sex Offenders? A Review of Sex Offender Typologies," *Aggression and Violent Behavior* 12 (2007): 508-518.

24 Ibid.

likely to be influenced by male offenders to abuse.[25] Various typologies have been proposed for juvenile sex offenders but no standard classification appears to have been adopted yet.

U.S. homicide rates exceed those of any comparable nations.[26] Violence and criminal behavior peaks in adolescence and young adulthood, and is preceded by risk factors such as aggression; exposure to violence; poor parenting; academic failure; negative peer influences; living in neighborhoods with a high concentration of poor residents; limited economic opportunities; access to firearms, alcohol and illicit drug use; high levels of transiency; and family disruption.[27] Research on homicide is better developed than research on multiple homicides, such as serial killing, spree killing, and mass murder.[28]

Application for the Department of Defense

Current knowledge from research could strengthen the Department of Defense's violence prevention efforts and assist with implementation of the recommendations offered in the Personnel Policies chapter of this repport. Known risk factors could be incorporated into the criteria for entry-level background checks and for citizenship and security clearances.

The integration of current knowledge into professional military education could provide supervisors and commanders the tools they need to make judgment calls in disciplinary cases, and when conducting performance and career counseling. This knowledge could also influence the types of adverse information that is recorded and shared throughout Service members' careers.

Research on workplace violence should guide improvements to mitigation efforts. Cutting-edge research on the pathways to terrorism should be used to update counterintelligence programs. Research on how cyberspace can foster violence should inform policy revisions for prohibited activities and cyber-related threats.

Dr. Greg Vecchi, who leads the FBI's Behavioral Science Unit, explained other ways that current information about offenders can be useful. For example, greater understanding of offender motivations and means can improve interactions with them, particularly when they make a direct threat.[29] This knowledge can also assist in the investigation of violent crimes or suspicious personnel. For example, a search of personal belongings might reveal items typical for certain types of offenders, such as literature advocating violence, personal manifestos, and souvenirs or documentation of crimes.

Academics have been developing violence risk assessment tools that the Department of Defense could employ or emulate. For example, the MacArthur Violence Risk Assessment Study produced a model to predict risk of violence among patients recently discharged from psychiatric facilities. Software

25 Gina Robertiello and Karen J. Terry, "Can We Profile Sex Offenders? A Review of Sex Offender Typologies," *Aggression and Violent Behavior* 12 (2007): 508-518.

26 Linda L. Dahberg, "Youth Violence in the United States: Major Trends, Risk Factors, and Prevention Approaches," *American Journal of Preventive Medicine* 14:4 (1998): 259-272.

27 Ibid.

28 An Crabbé, Stef Decoene, and Hans Vertommen, "Profiling Homicide Offenders: A Review of Assumptions and Theories," *Aggression and Violent Behavior* 13 (2008): 88-106; Matt DeLisi, Andy Hochstetler, Aaron M. Scherer, Aaron Purhmann, and Mark T. Berg, "The Starkweather Syndrome: Exploring Criminal History Antecedents of Homicidal Crime Sprees," *Criminal Justice Studies* 21:1 (2008): 37-47; Craig Dowden, "Research on Multiple Murder: Where Are We in the State of the Art?" *Journal of Police and Criminal Psychology* 20:2 (2008): 8-18.

29 Gregory Vecchi, Ph.D., Tiffany Hill, and Steve Conlon, FBI Behavioral Science Unit, FBI Academy, Quantico, VA, in discussion, Dec. 14, 2009.

incorporating this model was quite accurate in its assessment of whether patients fell into a low- or high-risk group for violence.[30] This software, called Classification of Violence Risk, is available for use with acutely hospitalized civil patients,[31] and suggests that the development of tools for other populations may be worth pursuing. The Danger Assessment Tool was created to identify women at risk of being killed by their intimate partners, and has had some success at doing so.[32] A full academic literature review would reveal other tools like these that the Department of Defense might use in part or in whole. The Department of Defense could also sponsor the development of a comprehensive risk assessment tool aimed at identifying those at risk for a wide range of violent behaviors, or for being the victim of violence.

30 John Monahan, Henry J. Steadman, Pamela Clark Robbins, Paul Appelbaum, Steven Banks, Thomas Grisso, Kirk Heilbrun, Edward P. Mulvey, Loren Roth, and Eric Silver, "An Actuarial Model of Violence Risk Assessment for Persons With Mental Disorders," *Psychiatric Services* 56:7 (2005): 810-815.

31 Monahan et al. 2005.

32 Jacquelyn C. Campbell, Daniel Webster, Jane Koziol-McLain, Carolyn R. Block, Doris Campbell, Mary Ann Curry, Faye Gary, Judith McFarlane, Carolyn Sachs, Phyllis Sharps, Yvonne Ulrich, and Susan A. Wilt, "Assessing Risk Factors for Intimate Partner Homicide," *National Institute of Justice Journal* 250 (2003): 14-19.

This page intentionally left blank.

Protecting the Force: Lessons from Fort Hood
The Report of the DoD Independent Review

Dr. Anthony C. Cain, PhD., Chief Editor

Captain Donald Gabrielson, U.S. Navy, Assistant Editor

Mr. Benjamin Bryant, Managing Editor

Mr. Thomas Zamberlan, Technical Editor

Mr. James Schwenk, Legal Advisor

Commander John Rickards, U.S. Navy

Commander Shawn Malone, U.S. Navy

Lieutenant Colonel James Clemonts, U.S. Army

Lieutenant Colonel Charlie Underhill, U.S. Air Force

Lieutenant Colonel Heather Kness, U.S. Army

Lieutenant Colonel Matthew Phares, U.S. Marine Corps

Major Jonathan Due, U.S. Army

Major Bryan Price, PhD., U.S. Army


DEPARTMENT OF THE ARMY
UNITED STATES OF AMERICA
1775
DEPARTMENT OF THE NAVY
UNITED STATES MARINE CORPS
DEPARTMENT OF THE NAVY
UNITED STATES OF AMERICA
DEPARTMENT OF THE AIR FORCE
UNITED STATES OF AMERICA
MCMXLVII
UNITED STATES COAST GUARD
SEMPER PARATUS
1790